Entwurf vom 05.07.2006

Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)

Änderung vom ….

Erläuternder Bericht

Inhaltsverzeichnis

1. Allgemeiner Teil

1.1 Ausgangslage nach geltendem Recht

1.1.1 Sicherheitspolitischer Auftrag

Die Instrumente zur Gewährleistung der inneren Sicherheit sind Staatsschutz und Polizei. Sie sind insoweit Gegenstand der Sicherheitspolitik, als sie der Bekämpfung von Gewalt dienen, die erhebliche Teile von Land und Bevölkerung beeinträchtigen kann. Bekämpfung von Gewalt nichtstrategischen Ausmasses ist Teil kantonaler Sicherheitspolitik. Bereits eingetretene Störungen werden primär durch die Kantone beseitigt.

Die sicherheitspolitischen Aufträge des Staatsschutzes und der Polizei sind die Folgenden:

- Der Staatsschutz trifft vorbeugende Massnahmen, um frühzeitig Gefährdungen durch Terrorismus, gewalttätigen Extremismus und verbotenen Nachrichtendienst sowie verbotenen Handel mit Waffen, radioaktiven Materialien und illegalen Technologietransfer zu erkennen. Der Staatsschutz unterstützt zudem die zuständigen Polizei- und Strafverfolgungsbehörden mit Erkenntnissen über die organisierte Kriminalität.
- Die hauptsächlich kantonaler Hoheit unterstehende Polizei sorgt für die öffentliche Sicherheit, Ruhe und Ordnung sowie die Bekämpfung der Kriminalität. Der Bund interveniert namentlich zur Bewältigung von Ereignissen, welche die Mittel und Möglichkeiten der Kantone übersteigen. Erfordert es die Lage, so übernimmt er die Führung.

1.1.2 Inland- und Auslandnachrichtendienst des Bundes

Die innere und äussere Sicherheit lassen sich kaum mehr strikte trennen; Sicherheit ist unteilbar. Gefahren und Risiken nehmen je länger, je mehr grenzüberschreitenden Charakter an, und Instabilität und Konflikte selbst in weit entfernten Gebieten können sich direkt und unmittelbar auf die innere Sicherheit der Schweiz auswirken.

Wie fast alle demokratischen Länder der Welt unterhält die Schweiz einen Inland- und einen Auslandnachrichtendienst. Der Strategische Nachrichtendienst (SND) im Departement für Verteidigung, Bevölkerungsschutz und Sport ist der Auslandnachrichtendienst der Schweiz.

Der Inlandnachrichtendienst der Schweiz ist der Dienst für Analyse und Prävention (DAP) im Bundesamt für Polizei, fedpol. Er ist beauftragt, die politischen Staatsleitungsorgane des Bundes und auch die Kantone frühzeitig mit Informationen über Gefährdungen im Bereich der inneren Sicherheit zu versorgen, damit rechtzeitig Abwehrmassnahmen getroffen werden können. Die Aufgaben des Inlandnachrichtendienstes werden im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120) und dem darauf beruhenden Verordnungsrecht geregelt.

Geht es bei den Gefährdungen um internationale Phänomene, die nicht nach dem territorialen Abgrenzungskriterium Inland – Ausland getrennt bearbeitet werden können, arbeiten die Nachrichtendienste eng zusammen, heute im Rahmen eines sog. Plattformmodelles in den Bereichen Terrorismus, organisierte Kriminalität und Proliferation.

1.1.3 Tätigkeit des Inlandnachrichtendienstes

a) Existenzbewahrende Dimension der Schutzaufgabe

Das permanente Beschaffen, Auswerten und Verbreiten von Nachrichten durch den DAP zielt darauf ab, die Staatslenkungsorgane über Bedrohungen zu informieren, die den Fortbestand des Landes, seiner freiheitlichen Gesellschaftsordnung und seiner demokratischen Institutionen gefährden können.

Diese, Gesellschaft und Nation als Ganzes erfassende Dimension des Staatschutzes bringt Artikel 1 des BWIS zum Ausdruck, indem er den Staatsschutz in den Dienst der Sicherung der rechtsstaatlichen und demokratischen Grundlagen der Schweiz sowie den Schutz der Freiheitsrechte stellt.

b) Aufgabengebiet des Inlandnachrichtendienstes

Um den Fortbestand einer Gesellschaft als Ganzes und die Sicherheit einer Vielzahl von Menschen ernstlich zu gefährden, braucht es Gleichgesinnte mit einem hohen Grad an destruktiver Entschlossenheit. Aus historischer Sicht liegen deshalb den staatsschutzrelevanten Gefährdungen in der Regel politisch-ideologische Motivationen zu Grunde. Demgegenüber obliegt aus historischer Sicht die Verfolgung der schwergewichtig pekuniär motivierten Kriminalität den Strafverfolgungsbehörden.

Nach heutigem Recht bearbeitet der DAP Gefährdungen durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst, verbotenen Handel mit Waffen und radioaktiven Materialien sowie verbotenen Technologietransfer. Weiter unterstützt er die zuständigen Polizei- und Strafverfolgungsbehörden, indem er ihnen Erkenntnisse über das organisierte Verbrechen mitteilt, namentlich wenn solche bei der Zusammenarbeit mit ausländischen Sicherheitsbehörden anfallen.

c) Präventiver Zweck

Die Abklärungen des DAP bezwecken, die zuständigen Behörden, namentlich die Führungsorgane im Bund und die Kantone, frühzeitig mit Informationen über die Sicherheitslage zu versorgen, damit rechtzeitig Gefährdungen erkannt (z.B. periodische Beurteilung der Bedrohungslage durch die politischen Behörden) und Massnahmen ergriffen werden können (z.B. Verhängung von Einreisesperren gegen ausländische Personen, welche die innere Sicherheit der Schweiz gefährden können oder Schutz von Personen und Einrichtungen). Das Handeln ist somit primär darauf ausgerichtet, mögliche Gefährdungen der Sicherheit der Schweiz abzuklären (präventiver Zweck der Verdachtsabklärung) und diese gegebenenfalls abzuwenden.

d) Massnahmen zur Informationsbeschaffung

Jede Gefahrenanalyse und darauf gestütztes Handeln basieren auf vielfältigen Informationen. Nur ein Teil der nötigen Informationen kann über allgemein zugängliche Wege beschafft werden. Die Beschaffung nicht öffentlicher Fakten ist eine zentrale Aufgabe eines Nachrichtendienstes. Dabei können in die nachrichtendienstlichen Produkte nicht mehr und nicht bessere Informationen einfliessen, als von Gesetzes wegen überhaupt beschafft und ausgewertet werden dürfen.

Wenn der Nachrichtendienst staatsschutzrelevante Gefahren und Bedrohungen aufdeckt, treffen nach Artikel 2 Absatz 2 BWIS die zuständigen Behörden von Bund und Kantonen die nötigen polizei- oder verwaltungsrechtlichen Massnahmen, um Gefahren oder bereits eingetretene Störungen abzuwehren.

Die im Rahmen der Prävention zulässigen Informationsbeschaffungsmittel sind in Artikel 14 Absatz 2 BWIS abschliessend aufgelistet. Danach können Personendaten 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.

Der Gesetzgeber hat in Artikel 14 Absatz 3 BWIS für den Inlandnachrichtendienst die Anwendung von Zwangsmitteln, wie sie im Rahmen von Strafverfahren zulässig sind, und das Beobachten in privaten Räumen ausgeschlossen. So ist beispielsweise der gesamte Kommunikationsbereich (Post, Telefon, Telefax, E-Mail) der präventiven Bearbeitung entzogen.

e) Strategischer Nachrichtendienst
Der Strategische Nachrichtendienst (SND) ist der Auslandnachrichtendienst der Schweiz und beschafft gestützt auf Artikel 99 Absatz 1 des Militärgesetzes vom 3. Februar 1995[1] (MG) zuhanden der obersten politischen und militärischen Führung, insbesondere für den Chef VBS, den Chef der Armee, den Sicherheitsausschuss des Bundesrates und die Lenkungsgruppe Sicherheit Informationen über das Ausland, die für die Sicherheit der Eidgenossenschaft bedeutsam sind, wertet diese aus und verbreitet sie. Er ist gemäss Artikel 99 Absatz 5 MG unmittelbar dem Chef des Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) unterstellt. Der SND verfügt über einen Grundauftrag, welcher von den drei im Sicherheitsausschuss des Bundesrates vertretenen Bundesräten unterzeichnet ist. Im Fokus der Beschaffungs- und Analysetätigkeit des SND stehen politische, wirtschaftliche, militärische und wissenschaftlich-technische Schwerpunktthemen. Darunter fallen insbesondere auch Bedrohungen durch Terrorismus, Organisierte Kriminalität und die Verbreitung von Massenvernichtungswaffen und deren Trägersystemen (Proliferation).

Die Aufgaben des SND werden in der Verordnung vom 26. September 2003[2] über die Nachrichtendienste im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VND) geregelt.

1.1.4 Abgrenzung der präventiven Staatsschutztätigkeit (Prävention) von der Polizeiaufgabe der allgemeinen Gefahrenabwehr

Die Tätigkeit des DAP ist auf den gesetzlichen Aufgabenbereich gemäss Artikel 2 BWIS beschränkt. In diesem Rahmen können nachrichtendienstlichen Erkenntnissen und Analysen sowohl Informationen über bevorstehende, als auch über bereits eingetretene Störungen der Sicherheit zu Grunde liegen.

Mit Blick auf bevorstehende Störungen der Sicherheit konzentrieren sich die Nachrichtendienste auf die Aufdeckung und rechtzeitige Warnung vor Gefahren, die

[1] SR **510.10**
[2] SR **510.291**

mit einer gewissen Wahrscheinlichkeit die öffentliche Sicherheit und Ordnung beeinträchtigen können. Sie handeln beispielsweise zur Verhinderung von Terroranschlägen durch zeitgerechtes Erkennen entsprechender Netzwerke und Verhinderung einschlägiger Aktivitäten. Da die Warnungen der Nachrichtendienste möglichst frühzeitig erfolgen sollen, müssen sie mit ihren Erhebungen vor dem Zeitpunkt einsetzen können, in welchem die entsprechenden Gefährdungen konkret und unmittelbar bevorstehen oder gar der Verdacht einer kriminellen Handlung besteht.

Demgegenüber ist das rechtzeitige Erkennen und Verhindern von Gewalt lokalen Ausmasses (z.B. Strassengewalt) Sache der kantonalen Polizeikorps, die im Rahmen der allgemeinen Gefahrenabwehr erst einschreiten dürfen, wenn entsprechende Gefährdungen konkret und unmittelbar bevorstehen. Bereits eingetretene Friedensstörungen werden von den kantonalen Korps gestützt auf den allgemeinen Polizeiauftrag beseitigt.

1.1.5 Abgrenzung der präventiven Staatsschutztätigkeit (Prävention) von der strafrechtlichen Repression

Für die Abgrenzung ist entscheidend, was die Behörden mit ihren Handlungen bezwecken (präventiver bzw. repressiver Zweck).

Sowohl präventive als auch repressive Tätigkeiten werden durch einen Verdacht ausgelöst.

Bei der präventiven Staatsschutztätigkeit geht es um die Abklärung des Verdachtes auf eine Gefährdung der Sicherheit der Schweiz oder ihrer Einwohner durch Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst, verbotenen Handel mit Waffen oder radioaktiven Materialien oder durch verbotenen Technologietransfer (präventiver Zweck).

Bei der Repression geht es um die Abklärung eines Verdachtes auf eine konkrete Straftat nach eidgenössischem oder kantonalem Recht (repressiver Zweck).

Das Ziel der präventiv ausgelegten Staatsschutztätigkeit ist die möglichst umfassende Enttarnung staats- und gesellschaftsbedrohender Strukturen sowie die Abwehr und Störung entsprechender undemokratischer Bestrebungen. Dazu beschaffen und bearbeiten die zuständigen Behörden Daten und Erkenntnisse über mögliche Gefährdungen der Sicherheit und treffen oder beantragen geeignete Abwehrmassnahmen.

Präventive Abklärungen erfordern in der Regel ein strategisches, auf dauerhafte Wirkung gerichtetes Vorgehen.

Anders verhält es sich bei der strafrechtlichen Repression. Hier wird der Staat zur justizförmigen Klärung eines Straftatverdachts mit Blick auf die Beurteilung von individueller Tatschuld tätig. Die Repression (Justiz und Kriminalpolizei) beinhaltet die Regelung des Konflikts zwischen der Rechtsgemeinschaft und dem Einzelnen, der grundlegende Normen der Gemeinschaft verletzt. Mit anderen Worten befasst sie sich mit der amtlichen Feststellung von menschlichem Verhalten im Zusammenhang mit einer konkreten Straftat oder einer strafbaren Vorbereitungshandlung dazu (somit Einzelfallbezogenheit).

Das Strafrecht hat zur Aufgabe, gewissen durch das Recht geschützten Gütern einen verstärkten Schutz zu verleihen. Der verstärkte Schutz geschieht einerseits dadurch, dass durch die Strafandrohung sowie durch das konsequente Verhängen und Vollstrecken von Strafen potenzielle Täter abgeschreckt werden. Anderseits wird bei gegebener Sachlage nachträglich zwangsweise in die Rechtsgüter des Täters eingegriffen (z.B. Freiheitsentzug). Hier lautet das Ziel Besserung, allenfalls Sicherung des Täters.

Nach dem Grundsatz der Legalität ist strafbar, wer eine Tat begeht, die das Gesetz ausdrücklich mit Strafe bedroht. Grundsätzlich gilt: Für's denken kann niemand henken. Unter dem Eindruck der Terrorismuswelle der siebziger Jahre wurden jedoch bereits Vorbereitungshandlungen zu bestimmten Kapitaldelikten (Art. 260bis StGB: vorsätzliche Tötung, Mord, schwere Körperverletzung, Raub, Freiheitsberaubung und Entführung, Geiselnahme, Brandstiftung) für selbständig strafbar erklärt und damit die Strafbarkeit ins planerische und vorbereitende Vorfeld einer Tatausübung verlagert. Ebenso wurde später zur Bekämpfung des organisierten Verbrechens schon die „blosse" Beteiligung an einer kriminellen Organisation unter Strafe gestellt (Art. 260ter StGB). Mit der Vorverlagerung der Strafbarkeit wird die Grenze zwischen Prävention und strafrechtlicher Repression zunehmend fliessend.

Die Verfolgung von Straftaten basiert auf einer Aufgabenteilung zwischen den Kantonen und dem Bund. Mit gerichtspolizeilichen Ermittlungen und der Verfolgung von Verbrechen im Kompetenzbereich des Bundes befassen sich die Bundesanwaltschaft (BA) und die Bundeskriminalpolizei (BKP). Sie wurden in den letzten Jahren deutlich gestärkt und ausgebaut (sog. Effizienzvorlage).

1.1.6 Abgrenzung der präventiven Staatsschutztätigkeit (Prävention) von den kriminalpolizeilichen Vorabklärungen

Die Abklärungen im präventiven Aufgabenbereich gemäss Artikel 2 BWIS erfolgen zur Gewinnung präventiv verwertbarer Erkenntnisse, so insbesondere zur Beurteilung der Bedrohungslage und dem Treffen präventiver Massnahmen (präventiver Zweck).

Anders verhält es sich bei den kriminalpolizeilichen Vorabklärungen. Sie dienen dazu, Klarheit über die Durchführung eines Strafverfahrens zu schaffen. Der Gesetzgeber hat im Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes (ZentG; SR 360) den Auftrag erteilt, Schwerstkriminalität gemäss Artikel 260ter bzw. 340bis des Schweizerischen Strafgesetzbuches (StGB; SR 311.0) zu erkennen, zu bekämpfen und zur Erfüllung dieser Aufgaben ein Informationssystem zu betreiben. Die Aufgabe wird heute von der BKP wahrgenommen. Die in diesem Zusammenhang zulässigen Informationsbeschaffungsmassnahmen entsprechen weitgehend denjenigen des bisherigen BWIS. Die einschlägigen Abklärungen der BKP gründen jedoch auf einem konkreten Tatverdacht und sind auf die Durchsetzung des Strafrechts gerichtet. Sie werden also mit repressivem Zweck durchgeführt, ein Kompetenzkonflikt mit den präventiven Behörden liegt nicht vor. Analoges gilt, wenn die BKP aus eigenem Antrieb ersten straftatverdachts-begründenden Informationen und Hinweisen nachgeht.
Allerdings bestehen dort Berührungspunkte, wo sich Abklärungen der Repression über strafbares Verhalten in einem konkreten Einzelfall mit präventiven Abklärungen

über Gefährdungen der Sicherheit der Schweiz überschneiden, weil die unter Verdacht stehende Person oder die mutmassliche Straftat gleichzeitig Gegenstand anders gelagerter präventiver Abklärungen ist. Mit anderen Worten kann zwar dieselbe Person oder Tat Abklärungsgegenstand bilden, dies jedoch unter völlig unterschiedlichen Blickwinkeln: Hier Erhärtung des Verdachts auf eine konkrete Straftat, dort Abklärung zur Beurteilung einer Gefährdung der inneren Sicherheit der Schweiz. In der Praxis wird im In- und Ausland oft beobachtet, dass längerdauernde nachrichtendienstliche Abklärungen kurzfristig von justizförmigen Verfahren überlagert werden. Durch dieses Nebeneinander von Repression und Prävention ergeben sich Mehrwerte und es zeitigt keine nachteiligen Folgen, wenn der gegenseitige Informationsaustausch spielt.

Hinsichtlich des Auskunftsrechts gelten für den präventiven Bereich und für die kriminalpolizeilichen Vorabklärungen ähnliche Regeln: Nach Art. 14 Abs. 4 ZentG und Art. 18 Abs. 6 BWIS muss registrierten Personen, die ein Auskunftsgesuch gestellt und aufgrund der Regelungen in den Art. 14 Abs. 2 ZentG und 18 Abs. 1 BWIS zunächst eine indirekte Auskunft des EDSB erhalten haben, nach Dahinfallen des Geheimhaltungsinteresses, spätestens aber bei Ablauf der Bearbeitungsdauer, von Amtes wegen auch noch direkt Auskunft erteilt werden. Mit diesem nachträglichen Rechtsschutz ist auch die Benachrichtigung über verdeckte Informationserhebungen verbunden.

1.1.7 Zusammenarbeit von DAP und BKP

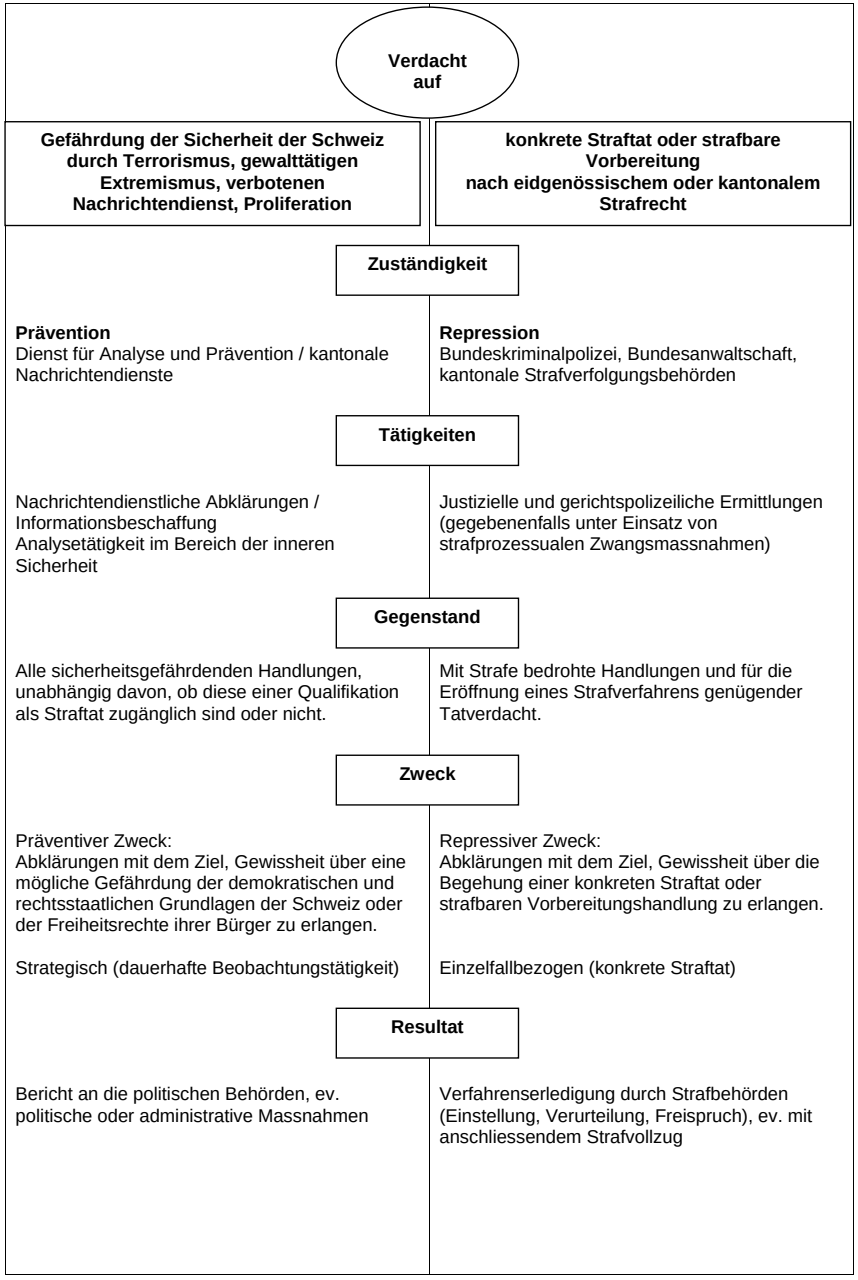
Die präventive Zweckausrichtung der Staatsschutztätigkeit schliesst nicht aus, dass nachrichtendienstliche Erkenntnisse an in- und ausländische Strafverfolgungsbehörden weitergegeben werden, wenn sie zur Verfolgung von Straftaten führen können. Gegenüber inländischen Strafverfolgungsbehörden besteht sogar eine Pflicht zur Weitergabe strafverfolgungsrelevanter Informationen (vgl. Artikel 17 Absatz 1 BWIS).

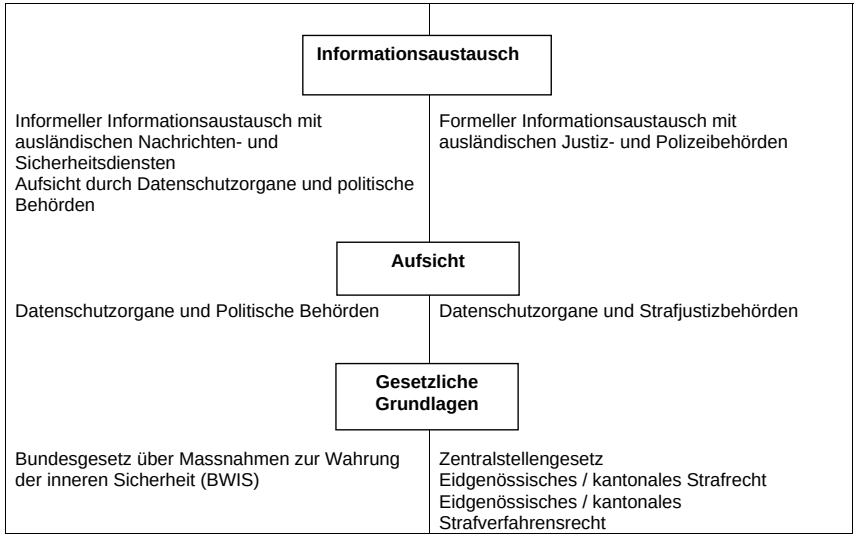
Sobald beim DAP im Rahmen seiner nachrichtendienstlichen Tätigkeit Hinweise anfallen, die geeignet erscheinen, einen Straftatverdacht zu begründen, gibt er diese an die zuständigen Strafverfolgungsorgane des Bundes oder der Kantone weiter. Je nach Konkretisierungsgrad der übermittelten Hinweise werden die Strafverfolgungsbehörden dann direkt zur Eröffnung eines Strafverfahrens schreiten oder aber Abklärungen zur weiteren Erhärtung oder Eingrenzung des konkreten Straftatverdachts veranlassen.

Umgekehrt verpflichtet das BWIS in Artikel 13 alle Polizeistellen und Strafverfolgungsorgane zur Auskunftserteilung und, wenn konkrete Gefährdungen der inneren oder der äusseren Sicherheit festgestellt werden, zur unaufgeforderten Meldung an den DAP. Weitere Meldungen erstatten die genannten Stellen aufgrund der allgemeinen Informationsaufträge nach Artikel 11 BWIS oder aufgrund von Aufträgen im Einzelfall.

1.1.8 Tabellarische Gegenüberstellung

Sowohl Repression, als auch Prävention nehmen sicherheitsrelevante Aufgaben wahr. Allerdings werden unterschiedliche Fragestellungen aus divergenten Blickwinkeln analysiert. Für die Abgrenzung ist entscheidend, zu welchem Zweck („repressiv" oder „präventiv") die Abklärungen erfolgen:





1.2 Sicherheitslage der Schweiz und ihre Risikofelder

Das BWIS regelt den präventiven Staatsschutz in der Schweiz. Es ist massgeblich von der sog. „Fichenaffäre“ geprägt und misst Fragen der Datenbearbeitung grosses Gewicht bei. Auf Informationsbeschaffungsmassnahmen, welche die Privatsphäre tangieren, wurde weitgehend verzichtet. Das Schwergewicht liegt auf der Begrenzung des Staatsschutzes und weniger auf seiner Schutzfunktion zu Gunsten der Öffentlichkeit. Diese Optik wurde denn auch ausdrücklich in der damaligen Botschaft festgehalten:

„Das Gesetz sieht die Informationsbearbeitung im Vorfeld der Strafverfolgung nur bei unbedingter Notwendigkeit vor. Der Bund nimmt damit ein gewisses Sicherheitsrisiko in Kauf,...“(Botschaft zum BWIS, BBl 1994 II 1229). Das Gesetz will die innere Sicherheit grundsätzlich mit dem bisherigen Instrumentarium von repressiven Massnahmen und Verfügungen wahren und vorbeugende Massnahmen nur für jene Bereiche vorsehen, in denen ernsthafte Gefahren für wesentliche Rechtsgüter abgewendet werden müssen. Es nimmt dabei in Kauf, dass gewisse Beeinträchtigungen der inneren Sicherheit erst durch nachträgliche Massnahmen behoben werden können.

Seit der Verabschiedung des BWIS hat sich die Bedrohungslage erheblich verschärft. Deshalb gilt es nun, die seinerzeit in Kauf genommenen Risiken an die veränderte Bedrohungslage anzupassen.

1.2.1 Terrorismus

Es gibt heute keine allgemeingültige, national oder international anerkannte Definition des Terrorismus. In der Schweiz sprach sich das Parlament im Jahre 2003 gegen die Einführung einer allgemeinen Terrorismus-Strafnorm aus. Eine indirekte

Definition auf Gesetzesstufe findet sich aber im 2003 in Kraft getretenen Artikel 260^{quinquies} StGB (Finanzierung des Terrorismus). Dieser stellt unter Strafe, „wer in der Absicht, ein Gewaltverbrechen zu finanzieren, mit dem die Bevölkerung eingeschüchtert oder ein Staat oder eine internationale Organisation zu einem Tun oder Unterlassen genötigt werden soll, Vermögenswerte sammelt oder zur Verfügung stellt."

Diese Umschreibung entspricht inhaltlich weitgehend jener der Verordnung vom 27. Juni 2001 über Massnahmen zur Wahrung der inneren Sicherheit (VWIS, SR 120.2; Art. 8 Abs. 1 Bst. a.), die terroristische Aktivitäten als Bestrebungen umschreibt „zur Beeinflussung oder Veränderung von Staat und Gesellschaft, die durch die Begehung oder Androhung von schweren Straftaten sowie mit der Verbreitung von Furcht und Schrecken verwirklicht oder begünstigt werden sollen". Die Umschreibung geht auf die Weisungen von 1992 des EJPD über die Durchführung des Staatsschutzes zurück, die wiederum in entscheidenden Belangen den Kriterien entspricht, die von der OECD in einer Definition von Terrorakten für versicherungstechnische Zwecke vorgeschlagen wurden: „Die Anwendung von Gewalt oder deren Androhung in Verbindung mit der politisch, ideologisch, religiös oder ähnlich motivierten Absicht, Regierungen zu beeinflussen oder zu destabilisieren oder Furcht in der Bevölkerung hervorzurufen".

Mit der vorliegenden Revision soll an dieser Rechtslage und der seit 1992 eingespielten Praxis im präventiven Staatsschutz nichts geändert werden. Die Definition der VWIS soll weiter gelten, während eine Definition im formellen Gesetz mangels internationaler Abstimmung weiterhin nicht opportun ist.

Die Sicherheitslage der Schweiz hat sich namentlich im Kontext der terroristischen Bedrohung in den letzten Jahren dauerhaft verschärft. Nach heutiger Beurteilung ist die Schweiz zwar kein primäres Ziel von islamistischem Terrorismus. Doch ist die allgemeine Gefahr für terroristische Aktionen in Europa gross, wovon auch die Schweiz – gleich wie andere westeuropäische Länder - betroffen ist. Der Bundesrat kam in der „Lage- und Gefährdungsanalyse nach den Terroranschlägen vom 11. September 2001", die am 26. Juni 2002 zuhanden des Parlaments verabschiedet wurde, zu dieser Beurteilung. Durch die anhaltend angespannte Sicherheitslage im Irak und im Nahen Osten muss unvermindert von einer erhöhten Gefährdung ausgegangen werden, insbesondere für Einrichtungen und Personen der USA und den mit ihnen verbündeten Staaten wie Grossbritannien, Italien, Spanien und Polen, aber auch Israel sowie - aufgrund ihrer grossen muslimischen Minderheiten - Deutschland und Frankreich.

Mit den Anschlägen von Istanbul (15. bzw. 20. November 2003), Madrid (11. März 2004) und London (7. bzw. 21. Juli 2005) zielte der islamistische Terror auch auf Europa. Die Londoner Selbstmordanschläge vom 7. Juli 2005 waren das erste islamistische Selbstmordattentat in Westeuropa. Westeuropa ist nicht länger nur Ruhe- oder Vorbereitungsraum. Die allgemeinen Terrordrohungen richten sich nicht mehr nur hauptsächlich gegen angloamerikanische und israelische Interessen, sondern gemeinhin gegen westliche Interessen, wozu aus fundamentalistisch - islamistischer Sicht z.B. auch die in der Schweiz angesiedelte UNO oder das IKRK gehören. Um die Botschaft des Schreckens zu verbreiten, suchen Terroristen Publizität. Völlig überraschende Sprengstoffanschläge auf grosse Menschenansammlungen sind ein Mittel dazu. Je besser die herkömmlichen Ziele

gesichert werden, umso grösser ist die Wahrscheinlichkeit, dass auf weniger stark gesicherte (sog. „weiche Ziele") ausgewichen wird. Schliesslich gilt es je länger, je mehr, dem im benachbarten Ausland (aufgrund grösserer Personalressourcen und weiter reichendem Instrumentarium) höheren Fahndungsdruck gegenüber Terrornetzwerken Rechnung zu tragen.

Die heutigen Terroristen bedienen sich aller Möglichkeiten. Um internationale Aufmerksamkeit zu erreichen, werden immer schrecklichere Ereignisse und blutigere Gewaltakte verübt. Derweil konventionelle Attentate – wie z.B. die Terroranschläge von New York (über 3000 Tote, tausende Verletzte) oder Madrid (191 Tote, ca. 1500 Verletzte) – an Grausamkeit kaum mehr entscheidend zu überbieten sind, wächst die Sorge vor nuklearen (atomaren oder radiologischen), biologischen oder chemischen Anschlägen.

Die Terroranschläge vom 11. September 2001 haben auch bestätigt, dass die modernen Industriegesellschaften weiterhin mit einem grossen Spektrum möglicher Gefährdungen - auch des klassischen Terrorismus - rechnen müssen. Bisherige sicherheitspolitische Handlungsmuster sind damit in Frage gestellt worden. Dies betrifft insbesondere der Einfluss von nichtstaatlichen Akteuren, die zunehmende Bedeutung von asymmetrischer Kriegführung sowie die präventive Informationsbeschaffung der Nachrichtendienste.

Die Bedrohung durch den nuklearen Terrorismus wird von Fachleuten – z.B. vom Generaldirektor der Internationalen Atomenergiebehörde – als real und aktuell beschrieben, wobei der radiologische Terrorismus in Form der sog. Dirty Bomb (Bombe mit konventionellem Sprengstoff, dem radioaktives Material beigefügt wird) im Vordergrund steht. Mag sich hier die Zahl der Verletzten und Toten zwar in Grenzen halten, ist dennoch von einer politisch, psychologisch und volkswirtschaftlich verheerenden Wirkung auszugehen. Das Schadenspotential eines nuklearen Anschlags kann auch der Einsatz von biologischem Terror haben, z.B. die Verbreitung von leicht übertragbaren Krankheitserregern wie dem Pockenvirus oder der Beulenpest. Einmal freigesetzt, dürfte eine solche „Waffe" nicht mehr kontrollierbar sein und könnte einen weltweiten, massenmordähnlichen Verlauf annehmen. Für Terroristen weniger geeignet scheinen schliesslich C-Waffen. Wenn ihnen auch lokal ein ähnlich verheerendes Vernichtungspotential wie A- oder B-Waffen einzuräumen ist, dürften sie in ihrer Wirkung auf ein bestimmtes Gebiet begrenzt bleiben.

Seit den Terroranschlägen von Madrid und London ist Westeuropa vom Ruhe- und Unterstützungsraum zu einem neuen Operationsfeld des islamistischen Terrorismus geworden. Bezeichnend für die heutige Situation sind sehr kleine (und deshalb personell nur schwer infiltrierbare), autonom handelnde und nicht hierarchisch organisierte Zellen, die teils völlig unabhängig voneinander agieren und sich gegenüber Aussenstehenden abschotten. Der Einsatz moderner Kommunikationsmittel sowohl zur internen Kommunikation, als auch zur Weiterverbreitung der Ideologie und damit Radikalisierung erfolgt fachkundig. Bei manchen fällt die Bereitschaft auf, bei einem Selbstmordattentat wie in London am 7. Juli 2005 als islamischer Märtyrer zu sterben. Hinzu kommt, dass sich die Täter immer häufiger aus im Zielland geborenen und dort aufgewachsenen, ideologisch bisher unauffälligen Nachkommen ausländischer Immigranten rekrutieren, welche mit den jeweiligen Verhältnissen vor Ort (und ebenso deren Schwachstellen) bestens

vertraut sind und den Eindruck einer guten Integration vermitteln. Weiter erschweren westliches Auftreten und die Verwendung nicht-europäischer Sprachen das Verständnis des Vorgehens. Im Übrigen ist mittlerweile das Know-how zur Verhinderung nachrichtendienstlicher Aufklärung beachtlich. Ohne Eingriffe in die Privatsphäre lassen sich Strukturen der geschilderten Art weder rechtzeitig erkennen, noch überwachen oder sonst wie genügend kontrollieren. Rückschlüsse aus einschlägigen Strafverfahren im Inland und aus im benachbarten Ausland gewonnenen Erkenntnissen zeigen deutlich, dass die Schweiz von „Al-Qaida“ unterstützenden Personen benutzt wird.

1.2.2 Verbotener Nachrichtendienst

Unter verbotenem Nachrichtendienst wird landläufig Spionage verstanden.

Ausländische Nachrichtendienste sind seit jeher in der Schweiz selber oder gegen schweizerische Interessen im Ausland aktiv. Interesse besteht an politischen, wirtschaftlichen und militärischen Informationen.

Nach der Überzeugung des Bundesrates gilt es zu differenzieren zwischen politischem und militärischem Nachrichtendienst auf der einen, und der Wirtschaftsspionage auf der anderen Seite. Bei der Wirtschaftsspionage sind in erster Linie die Unternehmen gefordert, geeignete Abwehrmassnahmen zu treffen.

Anders verhält es sich beim politischen und militärischen Nachrichtendienst. Hier sind adäquate staatliche Abwehrmassnahmen seit jeher unabdingbar.

Es fällt auf, dass seit dem Inkrafttreten des BWIS im Vergleich zu früher immer weniger mit Spionage befasste Personen im Einsatz enttarnt, Spionagestrukturen aufgeklärt und verbotener Nachrichtendienst wirksam verhindert werden kann. Der durch den Wegfall einschlägiger Verfahren entstandene Eindruck, die Schweiz sei davon gar nicht mehr oder bloss noch geringfügig betroffen, kann indessen nicht zutreffen. Denn nach den Erkenntnissen des DAP sind gewisse Länder mit einer grossen Zahl von Nachrichtendienstoffizieren unter diplomatischer Tarnung in der Schweiz präsent. Hinzu kommen Abklärungen privater internationaler Ermittlungsbüros und Detekteien, die nicht selten in (verdecktem) staatlichem Auftrag handeln.

Beim politischen und militärischen Nachrichtendienst wäre es unrealistisch davon auszugehen, dass die Tätigkeit ausländischer Nachrichtendienste mit dem Ende des kalten Krieges vorbei sei. Die von gewissen Ländern in der Schweiz stationierte grosse Zahl (sicher identifizierter oder mutmasslicher) Nachrichtendienstoffiziere belegt nachgerade die Weiterführung einschlägiger Aktivitäten. Ohne Zugang zum privatem Raum (mittels technischem Überwachungsgerät usw.) kann die schweizerische Abwehrbehörde jedoch wenig ausrichten, weil die Zielpersonen professionell darauf geschult und bestens dafür gerüstet sind, ihre Aktivitäten zu verheimlichen und zu vertuschen. Im Bereiche der Spionageabwehr machen sich die fehlenden Kompetenzen bei der Informationsbeschaffung je länger, je drängender bemerkbar.

1.2.3 Gewalttätiger Extremismus

Als gewalttätiger Extremismus gelten Bestrebungen von Organisationen, deren Vertreter die Demokratie, die Menschenrechte oder den Rechtsstaat ablehnen und

zum Erreichen ihrer Ziele Gewalttaten verüben, befürworten oder fördern (vgl. Artikel 8 Absatz 1 Buchstabe c VWIS).

Extremistische Aktivitäten bergen ein Gewaltpotenzial in sich und können, müssen aber nicht zwingend, die innere Sicherheit eines Landes bedrohen. Deshalb gilt es, potenziell gewalttätige Aktivitäten extremistischer Organisationen frühzeitig zu erkennen und zu verhindern.

Sowohl die rechtsextreme, als auch die linksextreme Szene der Schweiz bestehen aus vielen kleinen, zumeist miteinander vernetzten Gruppierungen. Man kann heute von einem Kern von insgesamt gegen 1000 Rechtsextremen in der Schweiz ausgehen; der linksextremen Szene sind rund 2000 Militante zuzurechnen. Auch ausländische extremistische Gruppen nutzen den grundrechtlich geschützten, relativ grossen Handlungsspielraum in der Schweiz.

Nach Auffassung des Bundesrates kann der aktuellen Bedrohungslage mit der heutigen Rechtslage genügend begegnet werden.

1.2.4 Verbotener Handel mit Waffen und radioaktiven Materialien sowie verbotener Technologietransfer (Proliferation)

Unter Proliferation versteht man die Weiterverbreitung von nuklearen, chemischen und biologischen Waffen, ihrer Trägersysteme (z.B. Raketen) sowie doppelt verwendbarer Güter, die für ihre Herstellung notwendig sind. Auch der dazu notwendige Technologietransfer fällt darunter.

Im Normalfall können ABC-Waffen im internationalen Waffenhandel nicht als Fertigprodukt erstanden werden. Daran interessierte Kreise sind deshalb gezwungen, eigene Forschungs-, Entwicklungs- und Produktionsstätten aufzubauen. Sie bedürfen dafür handelsüblicher Maschinen, Messgeräte und Materialien, die auch im zivilen Bereich an zahlreichen Stellen eingesetzt werden können (sog. Dual-use oder doppelt verwendbare Güter). So ist beispielsweise die Lieferung von Ersatzteilen für Tunnelbohrmaschinen im allgemeinen unproblematisch. Anders verhält es sich, wenn die Maschine zum Bau einer unterirdischen Fabrikationsanlage für chemische Waffen oder Raketen verwendet werden soll.

Die Entwicklung und Produktion von B- und C-Waffen ist im Vergleich zu Kernwaffen viel einfacher und kostengünstiger.

Für die Beschaffung des erforderlichen Know-hows können die unterschiedlichsten Mittel zum Einsatz gelangen (Abwerbung von Spezialisten, Gründung von Tarnfirmen, Übernahme von Herstellerfirmen der gewünschten Technologie, Import von Technologie unter Tarnung der Endverwendung und des Endverbrauchers, usw.).

Die Schweiz ist Signatarstaat aller internationalen Abkommen, die den Handel mit Massenvernichtungswaffen untersagen, und aller Verträge zur Rüstungskontrolle.

Die Aufdeckung des auf Nukleartechnologie spezialisierten Transfernetzwerkes des „Vaters“ der pakistanischen Atombombe, Dr. Abdul Qadeer Khan, zeigte nicht nur eindrücklich die hochkomplexe und professionelle Struktur solcher Netzwerke auf, sondern auch, dass die Schweiz ohne weiteres in solche Machenschaften

hineingezogen und ihre Infrastruktur gezielt für Beschaffungsaktivitäten benützt werden kann und wird. Dadurch drohen ihr auch erhebliche Reputationsrisiken.

Im Bereich des verbotenen Handels mit Waffen und radioaktiven Materialien sind hochkomplexe Netzwerke am Werk, welche oft international agieren (weshalb in den einzelnen Ländern im Regelfall nur Puzzleteile sichtbar werden). Die entscheidenden Absprachen und Vorgänge erfolgen nicht im öffentlichen, sondern diskret im privaten Raum. Nicht selten gehen mit solchen Geschäften auch sehr bedeutende Geldzahlungen einher, was die involvierten Personen zu noch mehr Verschwiegenheit und zum Einhalten von noch grösseren Vorsichtsmassnahmen veranlasst. In einer ersten Phase liegen erfahrungsgemäss bloss vage Verdachtselemente für eine Sicherheitsgefährdung vor, so beispielsweise wenn eine einschlägig bekannte Person in die Schweiz einreist, ohne dass jedoch der konkrete Grund der Reise bekannt ist oder dieser zu Zweifeln oder zu Besorgnis Anlass gibt. Die Abklärung eines sich auf bestimmte, aktuelle Tatsachen gründenden Verdachts, dass von den involvierten Personen oder Organisationen eine erhebliche Gefährdung der inneren oder äusseren Sicherheit der Schweiz ausgeht, ist im Proliferationsbereich ohne Möglichkeit der Überwachung der Geheim- und Privatsphäre durch den Nachrichtendienst so gut wie aussichtslos. Die bereits erwähnte Aufdeckung von Teilen des auf Nukleartechnologie spezialisierten Khan-Transfernetzwerkes belegt, dass schweizerisches Know-how (sei es infrastruktureller oder technischer Natur) gezielt genutzt wird.

1.2.5 Organisierte Kriminalität (OK)

Das organisierte Verbrechen ist global und kann mittelfristig zu einer der grössten Bedrohungen für Gesellschaft, Staat und Wirtschaft werden. Die Einnistung in das normale Geschäftsleben durch Geldwäscherei, Korruption sowie den Aufkauf von Firmen und Immobilien bedroht die wirtschaftliche und gesellschaftliche Stabilität. Aber auch die Staaten selbst, bzw. ihre Wirtschaftspolitik oder ihr Polizei- und Gerichtswesen, sind oftmals Infiltrationsziele der OK. Schwerpunkte der zum Teil untereinander vernetzten kriminellen Gruppierungen sind Drogen-, Menschen- und Waffenhandel, Korruption, Erpressung sowie die damit verbundene Geldwäscherei. Anlass zur Sorge geben zudem mögliche Verbindungen zu terroristischen Gruppierungen.

Hoch entwickelte und international stark vernetzte Volkswirtschaften bieten kriminellen Organisationen viele Möglichkeiten zur Infiltration und zum Waschen von Gewinnen.

Nach Auffassung des Bundesrates wurde der aktuellen Bedrohungslage mit dem in den letzten Jahren erfolgten Ausbau von BA und BKP (sog. Effizienzvorlage) ausreichend Rechnung getragen.

1.3 Beurteilung der Lücken zwischen Risikolage und Mittel

Wie der Bundesrat schon in seiner Lage- und Gefährdungsbeurteilung von 2002 festgestellt hat, hat sich die Sicherheits- und Gefahrenlage der Schweiz in den letzten Jahren sukzessive verschlechtert. Die Risiken haben sich namentlich durch die brutalen Terroranschläge islamistischer Täter deutlich akzentuiert. Die Täter zielen dabei nicht auf bestimmte Persönlichkeiten, sondern versuchen durch

rücksichtslose Anschläge gegen zivile Einrichtungen, möglichst viele Personen zu töten. Der Bundesrat ist überzeugt, dass derartigen Gewaltakten schon im Vorfeld begegnet werden muss, so dass ihre Vorbereitung bereits erkannt und damit die Anschläge verhindert werden können. Dazu sind Massnahmen zur Beobachtung gefährlicher Personen und Gruppen und eine optimale internationale Zusammenarbeit notwendig.

Die in Kraft stehenden, anerkanntermassen sehr zurückhaltenden gesetzlichen präventiven Möglichkeiten reichen für die Bewältigung der aktuellen Gefahrenlagen nicht aus. Manifeste Lücken bestehen vor allem in der Möglichkeit der Informationsbeschaffung und –bearbeitung.

So ist der Geheim- und Privatbereich ungeachtet der Gefährdungslage generell der Beobachtung entzogen; Treffen und Absprachen an privaten Orten können nicht festgestellt werden. Ebenso wenig kann heute die elektronische Kommunikation zwischen verschiedenen terroristischen Gruppierungen oder bestimmten Personen überwacht werden. Dies wirkt sich zunehmend negativ aus, weil die verschiedenen Personen und Gruppierungen nicht mehr hierarchisch kommandomässig strukturiert sind, sondern mehr oder weniger unabhängig agieren und nur durch elektronische Kommunikation oder Kuriere verbunden sind. Dies gilt besonders für internetbasierte Techniken, die heute der Prävention weitgehend entzogen sind.

Wo selbst diese Kommunikation fehlt, müssen die Staatsschutzbehörden durch getarnte menschliche Kontakte zu den entsprechenden Gruppen und Personen Nachrichten zu gewinnen suchen, um rechtzeitig gefährliche Absichten und Gefahren erkennen zu können. Dazu sind Tarnidentitäten nötig, die heute fehlen.

Ferner bestehen derzeit Lücken in den formellgesetzlichen Grundlagen für den Einsatz der Funkaufklärung sowohl im BWIS als auch im Militärgesetz. Der Bundesrat musste in den letzten Jahren vermehrt auf seine Verfassungskompetenzen zurückgreifen, um Personen Tätigkeiten zu verbieten, welche die Sicherheit der Schweiz oder ihre Beziehungen zum Ausland gefährdeten. Wenn solche Massnahmen regelmässig notwendig werden, so müssen sie auf Gesetzesstufe geregelt werden. Die Verfassungskompetenzen dürfen nur in ausserordentlichen Fällen zum Einsatz kommen.

1.4 Handlungsoptionen

Angesichts der verschärften Bedrohungslage, namentlich im Terrorismus- und Proliferationsbereich, besteht Handlungsbedarf. Ebenso wenig ist gegen die Schweiz gerichteter politischer und militärischer Nachrichtendienst tolerierbar. Es drängt sich auf, in diesen Bereichen das Sicherheitsrisiko zu verkleinern.

Deshalb ist zu prüfen, wie diesem Handlungsbedarf Rechnung getragen werden kann. In Betracht fallen

- das konsequente Ausschöpfen bestehender Möglichkeiten im Bereich des Strafrechts und des präventiven Staatsschutzes;
- die Verbesserung des Informationsflusses und der Koordination zwischen Repression und Prävention;

- der Ausbau des formellen und materiellen Strafrechts;
- der Ausbau des präventiven Staatsschutzes (Änderung BWIS).

1.4.1 Konsequentes Ausschöpfen bestehender Möglichkeiten im Bereich des Strafrechts und des präventiven Staatsschutzes

Einerseits bestehen keine konkreten Anhaltspunkte, dass die heutigen gesetzlichen Kompetenzen systematisch und in grösserem Umfang nicht korrekt ausgeschöpft würden. Anderseits lassen sich die zur Schliessung der Sicherheitslücken erforderlichen Informationen selbst mit einer noch so extensiven Auslegung und Anwendung des heutigen Rechts nicht genügend befriedigen. Eine konsequente Nutzung des Strafrechts zu Gunsten des BWIS wäre an sich wünschbar. Dies könnte etwa durch geringere Anforderungen für die Eröffnung von Strafverfahren oder mit einem deutlich grösseren Ressourceneinsatz erfolgen. Die bestehenden Lücken können jedoch mit derartigen Massnahmen alleine nicht geschlossen werden.

1.4.2 Verbesserung des Informationsflusses und der Koordination zwischen Repression und Prävention

Der DAP ist über die bei Bund und Kantonen im Bereich der inneren Sicherheit getätigten präventiven Abklärungen umfassend orientiert. Anders verhält es sich in Bezug auf die Erkenntnisse der Strafbehörden, wo der Wissenstand auf die von den genannten Behörden übermittelten Informationen beschränkt ist.

Es stellt sich deshalb die Frage, ob die heute bei der Prävention bestehenden Informationsdefizite mit einem optimalen Informationsfluss von Repression zu Prävention gelöst werden können. Dies muss jedoch bereits aus strukturellen Gründen verneint werden. Denn die Informationen repressiver Natur werden einzelfallweise erhoben und beschränken sich auf die im Rahmen von konkreten Strafverfahren zu bestimmten Straftatbeständen getätigten Ermittlungen. Demgegenüber sind die auf eine umfassende Beurteilung der Bedrohungslage und Ergreifung entsprechender Abwehrmassnahmen ausgerichteten Informationsbedürfnisse der Präventionsbehörde nicht nur viel umfassender und weiter gefasst, sondern auch strategischer Art und damit auf eine permanente Beobachtungstätigkeit ausgerichtet.

Die Verbesserung des Informationsaustausches zwischen BA, BKP und DAP ist eine permanente Aufgabe. Die Zusammenarbeit ist in Gesetzen, Verordnungen und Weisungen detailliert geregelt, die internen Abläufe sind festgelegt und werden regelmässig überprüft. Weitere Massnahmen sind im Gange. Bereits heute steht fest, dass die Lücken im Bereich der Inlandaufklärung selbst bei unterstellten zusätzlichen Verbesserungsmöglichkeiten bei weitem nicht geschlossen werden können.

1.4.3 Ausbau des formellen und materiellen Strafrechts

Hier ist zu prüfen, ob sich die Informationsdefizite des DAP mit einem Ausbau des materiellen (z.B. Strafnorm für „Hassprediger“) oder formellen (z.B. Zeugenschutzprogramme) Strafrechts und dem damit einhergehenden Informationsgewinn befriedigen lassen.

Dafür spricht, dass auf bestehende Strukturen und auf bestehendes Verfahrensrecht mit ausgebautem Rechtsschutz bei der Anordnung und Durchführung von strafprozessualen Zwangsmassnahmen zurückgegriffen werden kann. Weiter gibt es

zu vielen Fragen gefestigte Lehre und Rechtsprechung. Es steht mit anderen Worten ein funktionierendes System zur Verfügung.

Dagegen sprechen folgende Bedenken:

- Nachrichtendienste entfalten eine permanente Beobachtungstätigkeit, wobei sie sich primär auf die Enttarnung von Vorgängen und Strukturen beschränken. Bis zu deren vollständigen Aufdeckung besteht grundsätzlich kein Interesse, in das Geschehen unmittelbar einzugreifen.
- Repressive Abklärungen im Zusammenhang mit einer Straftat und das dabei zur Verfügung stehende Instrumentarium bezwecken grundsätzlich Anderes als präventive nachrichtendienstliche Abklärungen zur Informationsbeschaffung im Rahmen einer sicherheitspolitischen Lagebeurteilung oder allenfalls daraus abgeleiteter Abwehrmassnahmen.
- Mit dem Erlass des BWIS zog der Gesetzgeber bewusst eine Grenze zwischen Repression und Prävention, die in der Folge vom Bundesrat im Rahmen der Reorganisation des Bundesamtes für Polizei auch organisatorisch konsequent umgesetzt wurde. An diesem Konzept soll festgehalten werden.
- Wenn präventive Informationsbeschaffung mit repressivem Instrumentarium erfolgte, würde die Arbeitsweise der vormaligen Bundespolizei de facto wieder eingeführt und die Trennung in Frage gestellt.
- Für die Informationsbeschaffung mit repressivem Instrumentarium muss zumindest ein gerichtspolizeiliches Ermittlungsverfahren in die Wege geleitet werden. Verläuft dieses ergebnislos, bleibt die betroffene Person de facto gleichwohl häufig mit einem negativen Image belastet. Dies ist insbesondere dann der Fall, wenn das Verfahren der Öffentlichkeit nicht verborgen blieb. Daraus können sich weitere Konsequenzen mit möglichen Haftungsfolgen für die öffentliche Hand ergeben, so beispielsweise wenn aufgrund des negativen Image die wirtschaftliche Existenz einer Person ganz oder teilweise in Mitleidenschaft gezogen oder gar vollständig vernichtet wird.
- Eine Verlagerung der Strafbarkeit ins planerische Vorfeld einer Tat, die über die bei selbständig strafbaren Vorbereitungshandlungen nach Artikel 260bis und 260ter StGB bereits vorgenommene hinausgeht, widerspricht nicht nur der Systematik des StGB, sondern vermag – weil für andere Zwecke ausgerichtet – auch nicht die Lücken der präventiven Informationsbeschaffung zu schliessen.
- Repressives Handeln gründet auf einer Strafnorm. In der Norm ist das strafwürdige Verhalten präzise umschrieben. Soll eine Strafnorm breite, auf präventive Erkenntnisse gerichtete Untersuchungshandlungen zulassen, muss das strafbare Verhalten sehr weit gefasst werden. Damit verliert die Norm jedoch ihre Vorhersehbarkeit, d.h. für die einzelne Person ist nicht länger genügend vorhersehbar, wie sie sich verhalten muss, um gesetzestreu zu bleiben.
- Nach heutigem Recht setzt repressives Tätigwerden einen hinreichenden Verdacht auf Begehung einer strafbaren Tat voraus. Gerade daran mangelt es jedoch typischerweise beim Beginn von nachrichtendienstlichen Abklärungen. In einer ersten Phase bestehen bloss Annahmen und vage Hinweise. Hinzu kommt, dass Gefahren für die innere Sicherheit häufig auf den ersten Blick kaum als solche erkennbar und einschlägige Handlungen (noch) nicht strafrechtlich fassbar sind. Soll deshalb ein Straftatbestand geschaffen werden, der zeitlich früh einsetzende präventive Abklärungen erlaubt, muss praktisch auf ein Anfangsverdacht verzichtet oder dieser weit herabgesetzt werden. Verdachtslose

Strafverfahren stehen jedoch im Widerspruch mit dem Grundsatz der Bestimmtheit von Strafverfahren.

Alles in allem überwiegen die mit einem Ausbau des StGB einhergehenden Nachteile die einer solchen Lösung eigenen Vorteile deutlich.

1.4.4 Ausbau des präventiven Staatsschutzes (Änderung BWIS)

Die festgestellten Lücken beschlagen die präventive Gefahrenabwehr und damit in erster Linie den präventiven Staatsschutz. Da das BWIS die Aufgaben und Mittel des präventiven Staatsschutzes regelt, ist es der treffende Regelungsort. Im Übrigen kann auch hier auf ein bewährtes System mit bestehenden Strukturen zurückgegriffen werden.

Überdies sprechen folgende weitere Punkte für einen Ausbau des BWIS:

- Die Prävention ist ein von der Sicherheitspolitik gesteuertes Instrument: Es ist die Politik bzw. die Exekutive, die ihre Bedürfnisse im Rahmen des Gesetzes anmeldet und die entsprechenden Aufträge erteilt. Es ist die Politik bzw. die Exekutive, der ermöglicht werden soll, sicherheitspolitische Gefahren von nationalem Ausmass frühzeitig zu erkennen und in die politische Beurteilung mit einzubeziehen. Und schliesslich ist es wiederum die Politik bzw. die Exekutive, die u.a. gestützt auf die Erkenntnisse der eidgenössischen und kantonalen Sicherheitsbehörden ihre sicherheitspolitischen Entscheide trifft und dafür die politische Verantwortung trägt. Es ist deshalb sachgerecht, die festgestellten Lücken im präventiven Abwehrdispositiv im Rahmen des unter der Kontrolle und der Aufsicht der Politik stehenden BWIS zu schliessen.
- Für die Bekämpfung des Terrorismus und vergleichbarer Gefahren sollen alle verfügbaren Mittel eingesetzt werden, d.h. sowohl das repressive, als auch das präventive Instrumentarium gelangen zur Anwendung. Für die Früherkennung und Gefahrenabwehr, d.h. die Verhinderung von Terror- oder ähnlichen Anschlägen ist vorab die Prävention und damit die Arbeit der Nachrichtendienste gefordert.
- Ein Gefälle bei den jeweiligen nationalen Sicherheitsinstrumentarien führt zu unterschiedlichen Standards. Mit einer Annäherung einiger nachrichtendienstlicher Befugnisse an diejenigen verschiedener Nachbarländer soll verhindert werden, dass die Schweiz zu einem Raum geringerer Sicherheit wird.
- Mit einem Ausbau des BWIS wird die internationale Zusammenarbeit nachhaltig gestärkt.
- Von einem Ausbau des BWIS werden die strafprozessualen Grundsätze, wonach strafrechtlich motivierte Ermittlungen eines hinreichenden Tatverdachts bedürfen und wonach strafwürdiges Verhalten für die Rechtsunterworfenen ausreichend vorhersehbar sein muss, nicht tangiert.
- Der Ausbau der Prävention ermöglicht dauerhafte und vertiefte Erkenntnisse über schwerstkriminelle Bereiche. Diese Erkenntnisse kommen den punktuell agierenden repressiven Organen vollumfänglich zu Gute und ermöglichen ihnen den zielgerichteten Einsatz ihrer Ressourcen.
- Durch gezielte nachrichtendienstliche Abklärungen und entsprechende frühzeitige Massnahmen können gravierende Straftaten verhindert, in vielen Fällen auf die zeit- und ressourcenaufwändige Eröffnung eines Strafverfahrens verzichtet und dadurch die Strafverfolgungsbehörden wirksam entlastet werden.

1.4.5 Total- oder Teilrevision?

Es bleibt zu klären, ob das BWIS für die anstehenden Gesetzgebungsarbeiten einer Totalrevision unterzogen werden muss oder ob sich die Arbeiten im Rahmen einer Teilrevision vornehmen lassen. Aus folgenden Gründen wird einer Teilrevision der Vorzug gegeben:

- Zur Zeit ist noch offen, was mit den im Rahmen von BWIS I (Bekämpfung von Gewalt an Sportveranstaltungen) befristet vorgeschlagenen Regelungen nach Ablauf ihrer Geltungsfrist (2009) geschehen soll.
- Die im Rahmen von BWIS II angestrebten Änderungen beinhalten zwar rein zahlenmässig vergleichsweise viele Gesetzesartikel, beschränken sich aber in materieller Hinsicht auf bloss wenige Themen mit dem klaren Schwerpunkt der Informationsbeschaffung mit besonderen Mitteln.
- Die angestrebten Änderungen lassen sich gesetzessystematisch zwar nicht ideal, aber in vertretbarer Weise in die bestehende Gliederung integrieren.
- Beim BWIS bleibt auch nach den Gesetzgebungspaketen BWIS I und II Anpassungsbedarf bestehen, so vor allem im Bereiche der Personensicherheitsprüfungen.
- Zusammenfassend scheint es deshalb klar vorteilhafter, vorderhand mit einer Totalrevision noch zuzuwarten bzw. eine solche später vorzunehmen.

1.5 Hängige Gesetzgebungsprojekte im Bereich der inneren Sicherheit

Die Gesetzgebung im Bereich der inneren Sicherheit befindet sich in einem ständigen Anpassungs- und Erneuerungsprozess. Zur Zeit werden zahlreiche internationalen Vereinbarungen, Gesetze und Verordnungen neu geschaffen oder revidiert. Eine Prüfung ergab jedoch, dass zwischen diesen Projekten und dem vorliegenden Gesetzgebungspaket keine relevanten Schnittstellen bestehen (vgl. Anhang 1).

Die vorliegende Revision bezweckt in erster Linie die Verbesserung der Informationsbeschaffung für die sicherheitspolitische Lagebeurteilung und daraus abgeleiteter Massnahmen. Als solches beeinflusst sie massgeblich die Steuerung der gesamten Gefahrenabwehr und zeitigt mittelbare Auswirkungen auf das formelle und materielle Strafrecht.

Die Prüfung der Anpassung der Rechtsgrundlagen für den SND ist im Gange.

1.6 Rechtsvergleich und Verhältnis zum europäischen Umfeld

1.6.1 Allgemeines

Die vorbestehenden und im Nachgang zu den Terroranschlägen vom 11. September 2001 erlassenen ausländischen Gesetzgebungen können angesichts der unterschiedlichen Gefährdungslagen, Rechtssysteme (jeweilige Funktion von Exekutive, Judikative und Legislative) und der landesspezifischen Erfahrung mit dem Terrorismus in den jeweiligen Staaten (z.B. Spanien / ETA) nicht unbesehen auf die Schweiz übertragen werden.

Die Zunahme der terroristischen Bedrohung hat generell zu einer verstärkten Zusammenarbeit unter den Nachrichtendiensten der internationalen Gemeinschaft geführt. Diese hat die Notwendigkeit erkannt, gemeinsam im Kampf gegen den Terrorismus zu handeln und die internationale Zusammenarbeit in diesem Bereich zu institutionalisieren. So dient beispielsweise die vom „Club de Berne“ geschaffene „Gruppe für Terrorismusbekämpfung“ (Counter Terrorist Group / CTG) als Schnittstelle zwischen der EU und den Leitern der Sicherheits- und Nachrichtendienste der Mitgliedsstaaten.
Das Schweizerische Institut für Rechtsvergleichung (SIR) verglich Anfang 2003 und Mitte 2005 die rechtlichen Grundlagen der inneren Sicherheit in den wichtigsten europäischen Ländern.
Die Gesetzgebung in allen nachfolgend erwähnten Ländern ist geprägt durch die Ereignisse des 11. Septembers 2001 in den USA.

Die verschiedenen Staatsstrukturen und die rechtlichen Handlungsmöglichkeiten unterscheiden sich von Staat zu Staat. Es ist deshalb nicht einfach, klare Vergleiche und Schlussfolgerungen für die Schweiz zu ziehen. Im Folgenden werden die gesetzlich geregelten Massnahmen und Kompetenzen in ausgewählten Ländern sowie den jeweils vorhandenen Rechtsschutz bzw. das Kontrollsystem vereinfacht in zwei Grafiken dargestellt. Die ausführlichen Erklärungen dazu befinden sich im Anhang. Das Fehlen einer ausdrücklichen gesetzlichen Regelung bedeuten dabei nicht notwendigerweise, dass die erwähnte Massnahme im betreffenden Land nicht zur Anwendung kommt. Sie wird möglicherweise als nicht regelungsbedürftig oder in anderen Regelungen miterfasst betrachtet.

1.6.2 Rechtsvergleich

Rechtsvergleich mit dem Ausland

Massnahme	Repression/Strafverfolgung	Prävention
Funkaufklärung (Exploration radio) Art. 14a-E		Deutschland, Frankreich, Italien, Niederlande
Entschädigung von Informanten (Dédommagement des informateurs) Art. 14b E-	Frankreich, Italien	Italien, Frankreich,
Schutz von Informanten (Protection des informateurs) Art. 14c E	Österreich, Deutschland, Frankreich, Italien	Österreich, Deutschland, Frankreich, Niederlande
Tarnidentität (Identité d'emprunt) Art. 14d E-	Österreich, Deutschland, Frankreich, Italien, Niederlande	Österreich, Deutschland, Frankreich, Niederlande
Überwachung des Brief-Post- und Fernmeldeverkehrs (Surveillance de la correspondance par poste et télécommunication) Art. 18k E	Österreich, Deutschland, Frankreich, Italien, Luxemburg, Niederlande	Deutschland, Frankreich (nicht Postüberwachung), Italien, Luxemburg, Niederlande
Observierung von privaten Räumen (Observation secrète d'un lieu qui n'est pas librement accessible au public) Art. 18l E	Österreich, Deutschland, Frankreich, Italien, Luxemburg, Niederlande	Österreich, Deutschland, Frankreich, Italien, Niederlande
Eindringen in elektronische Systeme (Perquisition secrète dans un système informatique) Art. 18m E	Deutschland, Frankreich, Luxemburg, Niederlande	Frankreich, Niederlande

Verbot bestimmter Tätigkeiten gegen Einzelpersonen oder Gruppen (Interdiction d'activités dangereuses pour la sûreté intérieure ou extérieure) Art. 18n E	Österreich, Deutschland, Italien, Luxemburg, Niederlande	Frankreich, Deutschland, Österreich

Rechtsschutz und Institutionelle Kontrollen im Ausland

Länder	Ordentliche Kontrolle	Besondere Kontrolle
Deutschland	**Allgemein:** Oberaufsicht des Datenschutzbeauftragten, Parlamentarische Kontrolle; Verpflichtungsklage beim Verwaltungsgericht	**Überwachung des Brief-Post- und Fernmeldeverkehrs:** Antrag durch Präsident des BfV oder Vertreter, Anordnung Bundesministerium; Überprüfungsinstanz: G 10- Kommission. Ausnahme: Gefahr in Verzuge, dann sofortiger Vollzug, nachträgliche Information der Kommission. **Tarnidentität:** Zustimmung des Bundesministers des Innern
Österreich	Möglichkeit der Beschwerde bei Datenschutzkommission, beim Verwaltungsgerichts- oder Verfassungsgerichtshof	**Allgemein:** Kontrolle des Rechtschutzbeauftragten; parlamentarische Kontrolle, Sicherheitsbehörden informieren Bundesminister für Inneres unverzüglich; **Verdeckte Ermittlung und verdeckter Einsatz von Bild- und Tonaufzeichnungsgeräten**: Begleitete Kontrolle durch Rechtschutzbeauftragten;
Frankreich	Einsichtsgesuche an „Commission nationale de l'information et des libertés“ (CNIL)	**Überwachung des Brief Fernmeldeverkehrs:** Antrag durch Verteidigungsministers, des Innenministers und des Ministers für Zollwesen oder ihrer Stellvertreter; Anordnung durch Premierminister oder zweier durch ihn ernannter Personen, Überprüfungsinstanz: Verwaltungsunabhängige „Commission nationale de contrôle des interceptions de sécurité„
Italien	Regierung liefert dem Parlament pro Semester ein Rechenschaftsbericht über die Aktivitäten der Dienste Datenschützer(Garante per la protezione die dati personali) übt Kontrolle der gesammelten Daten aus	**Überwachung des Brief-Post- und Fernmeldeverkehrs** Antrag durch den Ministerpräsidenten, Einwilligung des Richters. Ministerpräsident kann seine Befugnisse an die Dienste delegieren; Anordnung durch Staatsanwaltschaft. Bei Gefahr in Verzug sofortige Anordnung. Spätestens nach 24 Stunden muss dem Richter auf dem ordentlichen Weg die Bewilligung eingeholt werden. Richter muss innerhalb von 48 Stunden über den Antrag entscheiden.
Luxemburg	Parlamentarischen Kontrollkommission; Aufsichtskontrolle der Daten durch den Generalstaatsanwalt oder einer seiner Delegierten und zwei vom Minister gewählten Vertreter einer Spezialkommission; Oberste Datenschutzstelle (ANS) wacht über Sicherheit der klassifizierten Daten	**Überwachung des Brief-Post- und Fernmeldeverkehrs:** Antrag durch SRDE im Einverständnis einer Spezialkommission; Anordnung durch Direktor der Telekommunikationsdienste, welcher die Abhörungen durch eine dafür geschaffene Stelle vollziehen und kontrollieren lässt. Die parlamentarische Kontrollkommission wird alle sechs Monate über die durchgeführten Massnahmen betreffend die Telefonüberwachung informiert
Niederlande	Aufsichtskommission; unabhängiger Ombudsmann. Parlamentarischen Aufsichtskommission	**Überwachung des Brief-Post- und Fernmeldeverkehrs:** Antrag durch Chef AIVD und MIVD, Anordnung durch Innenminister. Bei Gefahr in Verzug, ist eine nachträgliche Genehmigung erlaubt, wenn diese so schnell wie möglich eingeholt wird,

	Tarnidentität: Briefe Dritter öffnen erlaubt, sofern das Bezirksgericht Den Haag einem Antrag des Chefs der Dienste entspricht	**Observierung:** Allgemein bei schriftlicher Einwilligung des zuständigen Ministers. Observation privater Räume. in Absprache mit dem Innenminister oder dem Chef der Dienste erlaubt.

1.6.3 Vergleich mit der Schweiz

Die Sicherheitsstrukturen und die rechtlichen Handlungsmöglichkeiten der Sicherheitsbehörden unterscheiden sich zwar von Staat zu Staat. Dennoch ergibt sich aus dem Rechtsvergleich, dass die heutigen schweizerischen Präventionsmassnahmen und die verfügbaren Ressourcen deutlich unter den Möglichkeiten liegen, die zahlreichen westeuropäischen Ländern zur Verfügung stehen.

Damit können gefährliche und international spürbare Lücken entstehen. Dies kann eine illegale Nachrichtenbeschaffung ausländischer Behörden auf Schweizergebiet zur Folge haben. In mehreren Fällen ist dies bereits geschehen.

Eine ungenügende Fähigkeit zur internationalen Zusammenarbeit kann zudem dazu führen, dass sich die Schweiz selber schadet, weil die Informationen nicht mehr so bereitwillig ausgetauscht werden. Das könnte zu einer nochmaligen Schwächung der schweizerischen Terrorabwehr führen.

Die Erfahrung der letzten Anschläge zeigt, dass die Netzwerke des Terrorismus bei Brüchen im Informationsaustausch viel zu spät erkannt werden können. In Fällen verhinderter Terroranschläge kamen Informationsbeschaffungsmittel zum Einsatz, die in der Schweiz heute präventiv nicht zur Verfügung stehen. So beispielsweise beim geplanten Attentat auf den Weihnachtsmarkt von Strassburg im Jahre 2000, bei der Entdeckung des Rizin-Pflanzengift-Labors in London (2003), bei der Aufdeckung des islamistischen Hofstad-Netzwerkes in Holland (2003) oder beim verhinderten Anschlag auf die Einweihung des jüdischen Kulturzentrums durch die Neonazigruppe „Kameradschaft Süd“.

Die Schweiz muss in der Lage sein, einen minimalen de-facto Standard der europäischen Staaten zu erreichen. Auf weitergehende Massnahmen wird vorläufig verzichtet.

1.7 Die vorgeschlagene Neuregelung

Die Gesetzesrevision zielt auf die Umsetzung der Folgerungen, die sich aus der am 26. Juni 2002 zuhanden des Parlamentes verabschiedeten „Lage- und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001“ und aus den parlamentarischen Vorstössen nach dem 11. September 2001 ergeben.

Um dieses Ziel zu erreichen, soll einerseits das bei der Beschaffung von Informationen zum Einsatz gelangende nachrichtendienstliche Instrumentarium wirksamer gestaltet und dem europäischen Standard angenähert werden. Beschränkt auf die Abwehr von Terrorismus, verbotenem politischen oder militärischem Nachrichtendienst und verbotenem Handel mit Proliferationsgütern (Weiterverbreitung von Massenvernichtungswaffen) sollen die Behörden und

Verwaltungseinheiten des Bundes und der Kantone in konkreten Fällen zur umfassenden Auskunftserteilung verpflichtet werden. Unter den nämlichen Voraussetzungen sollen auch gewerbliche Transporteure auskunftspflichtig werden, soweit von ihnen ohnehin bereits erhobene Daten benötigt werden. Weiter soll unter sehr strengen Voraussetzungen und im Sinne einer „ultima ratio“ besondere Mittel zur Informationsbeschaffung eingesetzt werden können. Wiederum beschränkt auf die Bereiche Terrorismus, verbotener politischer oder militärischer Nachrichtendienst und Proliferation soll bei gegebener Verdachtslage das Überwachen des Post- und Fernmeldeverkehrs, das Beobachten an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät, sowie das geheime Durchsuchen von Datenbearbeitungssystemen ermöglicht werden.

Der Einsatz von besonderen Mitteln zur Informationsbeschaffung wird einer doppelten Kontrolle unterstellt: Das Verfahren wird mit einem Antrag des Bundesamtes für Polizei eingeleitet. In der Folge prüft das Bundesverwaltungsgericht die Rechtmässigkeit des Antrages. Fällt diese positiv aus, geht der Antrag zur Prüfung nach staatspolitischen Gesichtspunkten an den Vorsteher oder die Vorsteherin des EJPD, der bzw. die den Vorsteher oder die Vorsteherin des VBS in seiner / ihrer Rolle als Vorsitzende(r) des Sicherheitsausschusses des Bundesrates konsultiert. Bei Einigkeit entscheidet der Vorsteher oder die Vorsteherin des EJPD abschliessend über den Antrag; bei Differenzen entscheidet der Bundesrat.

Die Überwachung muss der betroffenen Person nach Beendigung der Operation mitgeteilt werden; vorbehalten bleiben im Einzelfall höher zu gewichtende öffentliche Interessen sowie Interessen zum Schutz von Dritten. Über Ausnahmen von der Mitteilungspflicht befindet der Departementsvorsteher oder die Departementsvorsteherin EJPD.

Die Kompetenz des Bundesrates, einer Person, Organisation oder Gruppierung eine bestimmte Tätigkeit zu verbieten (z.B. Geldsammlung), soweit die Tätigkeit mittelbar oder unmittelbar dazu dient, terroristische oder gewaltextremistische Umtriebe zu propagieren, zu unterstützen oder in anderer Weise zu fördern und die innere oder äussere Sicherheit der Schweiz konkret gefährdet, soll an den Vorsteher des EJPD delegiert und gesetzlich geregelt werden. Die Kompetenz, Organisationen zu verbieten, verbleibt wie bis anhin beim Bundesrat.

Im übrigen soll die Möglichkeit der Inanspruchnahme von Informanten bzw. die Natur der ihnen gewährten finanziellen Entschädigung (weder AHV-, noch steuerpflichtiges Einkommen) auf eine formellgesetzliche Grundlage gestellt und daneben die Möglichkeit geschaffen werden, solche Personen bei Bedarf zu schützen. Um bei der Informationsbeschaffung den Schutz von Informanten und Mitarbeitenden des DAP sicherzustellen, wird auch die Möglichkeit zur Legendierung (Tarnidentität) geschaffen. Schliesslich wird die (seit langem bewährte) Lagedarstellung durch das Bundeslagezentrum gesetzlich geregelt und mit einer Ergänzung im Bereiche der Personensicherheitsprüfungen (sog. „Clearing“) wird sichergestellt, dass Schweizerinnen und Schweizer, gleich wie hier wohnhafte ausländische Personen, auch inskünftig die Möglichkeit haben, an klassifizierten Projekten des Auslandes mitzuarbeiten.

1.8 Umsetzung

Für die Umsetzung der Massnahmen soll weitestgehend auf die bestehenden eidgenössischen (Bundesverwaltungsgericht, Dienst für Analyse und Prävention) und

kantonalen Strukturen (kantonale Nachrichtendienste) aufgebaut werden. Für Bundesverwaltungsgericht, Dienst für besondere Aufgaben UVEK (für die Post und Fernmeldeüberwachungen) und die rechtliche, operationelle und administrative Umsetzung der neuen Beschaffungsmöglichkeiten sowie für die Verarbeitung der Resultate bei fedpol ist mit insgesamt rund 40 Stellen zu rechnen. Diese sollen durch EJPD-interne Kompensationen geschaffen werden.

Der Stellenmehrbedarf ist somit schwergewichtig auf folgende Bereiche zurückzuführen:

- Stärkung der operationellen Strukturen, insbesondere der mit der Informationsbeschaffung und –bearbeitung befassten polizeilichen Stellen (Polizisten, Dolmetscher, Techniker, operative Analytiker);
- Stärkung der datenverarbeitenden Strukturen, insbesondere der Datenerfassung, der Qualitätssicherung und beim Verkehr mit dem Ausland;
- Stärkung Nachrichtendienst fremder Strukturen wie des DBA UVEK (Technik und Administration) oder des Bundesverwaltungsgerichts (Sekretariat).

Die zusätzlichen Kompetenzen können demnach weiterhin mit einem engen Ressourcenansatz umgesetzt werden.

2. Besonderer Teil

2.1 Allgemeine Systematik

Die Einführung von besonderen Mitteln zur Informationsbeschaffung bedarf einer anderen Regelung als jener, die für die bisherigen einfachen Mittel gilt. Das erfordert eine Änderung in der Systematik des Aufbaus des Gesetzes. Das Gesetz wird um ein Kapitel mit zwei Abschnitten erweitert. Im ersten Abschnitt werden die auf die neuen Mittel allgemein anwendbaren Regeln statuiert. Der zweite Abschnitt ist den besonderen einzelnen Mitteln der Informationsbeschaffung und ihrer Anwendung gewidmet. Die Einführung dieses Kapitels bedingt eine Änderung des allgemeinen Aufbaus des Gesetzestextes.

2.2 Artikel 2, Absatz 4, Buchstaben b^{bis} und b^{ter}

Das geltende Gesetz zählt die vorbeugenden Massnahmen in Artikel 2 Absatz 4 abschliessend auf. Diese Auflistung ist mit den neu eingeführten, in Kapitel 3a geregelten besonderen Mitteln der Informationsbeschaffung (Buchstaben b^{bis}) bzw. dem Tätigkeitsverbot (Buchstaben b^{ter}) gemäss Kapitel 3b zu ergänzen.

2.3 Artikel 7, Absatz 2, dritter Satz

Nach Artikel 7 Absatz 2 BWIS erfüllen die Kantone die Aufträge nach diesem Gesetz selbständig. Müssen mehrere Kantone mitwirken oder ist Gefahr in Verzug, kann das Bundesamt die Leitung übernehmen. Diese Kompetenz soll ergänzt werden: Das Bundesamt kann den Austausch von Informationen koordinieren, wenn dadurch die Arbeit bei Bund und Kantonen erheblich erleichtert werden kann. Es geht also um die Sicherstellung eines koordinierten Informationsaustausches durch das Bundesamt zwischen (kantonalen) Verwaltungseinheiten, die originär zuständig sind und es auch bleiben. Der Begriff Koordination soll den kooperativen Charakter der Massnahme verdeutlichen. Mit dem Kriterium der Massgeblichkeit wird sichergestellt, dass beim gegenseitigen Informationsaustausch ein klares Plus resultieren muss. Die durch das Bundesamt sichergestellte Kooperation soll also das Informationsaufkommen aller beteiligten Stellen erheblich verbessern. Im Übrigen handelt es sich um eine „kann“ Bestimmung; Pflicht zur Übernahme der Koordination besteht keine.

Öffentliches Interesse und Verhältnismässigkeit

Mit der zunehmenden Internationalisierung der terroristischen und gewaltextremistischen Ideologien und ihrer militanten Anhängerschaft wird die präventive Gefahrenabwehr immer schwieriger. Deshalb rechtfertigt es sich, die koordinierende Funktion des Bundesamtes bei der Wahrnehmung der ihm gesetzlich übertragenen Aufgaben anzupassen. Um eine entsprechende Gefährdung frühzeitig zu erkennen, sind umfassende Kenntnisse der komplexen, oft grenzüberschreitenden Vorgänge und personellen Verflechtungen unabdingbar. Als ebenso wichtig erweist sich in der Regel ein intensiver Informationsaustausch mit ausländischen Partnerbehörden. Die nun vorgeschlagene Koordination respektiert im Übrigen das verfassungsmässige Subsidiaritätsprinzip, das für die Aufgabenteilung zwischen Bund und den Kantonen massgebend ist (vgl. den neuen Artikel 5a BV, welcher im November 2004 vom Volk und den Ständen angenommen wurde und voraussichtlich am 1. Januar 2008 in Kraft treten wird).

2.4 Kapitel 3 Allgemeine Informationsbeschaffung und -bearbeitung

Bedingt durch die neue allgemeine Systematik des Gesetzes wird der bisherige 3. Abschnitt zum Kapitel 3.

Die Überschrift des neuen Kapitels 3 wird geändert, um den Unterschied zwischen der Allgemeinen Informationsbeschaffung und der Besonderen Informationsbeschaffung (Kapitel 3a) besser hervorzuheben. Die Allgemeine Informationsbeschaffung ist identisch mit der heute zulässigen Informationsbeschaffung. Sie greift kaum in Grundrechte ein und entspricht dem liberalen präventivpolizeilichen Verständnis des Gesetzgebers von 1997 (z.B. Auswerten öffentlich zugänglicher Quellen oder Beobachten von Vorgängen an öffentlichen und allgemein zugänglichen Orten). Folgerichtig orientieren sich die zulässigen Möglichkeiten in erster Linie an der Amtshilfe unter Behörden (vgl. die Auskunftspflichten kantonaler Behörden oder bestimmter Bundesbehörden).

Das Kernstück des heutigen BWIS ist die Regelung der Informationsbearbeitung. Daran ändert die vorliegende Revision nichts. Die einschlägigen Regeln gelten weiterhin und auch für die mit den besonderen Mitteln der Informationsbeschaffung erhobenen Daten, soweit in Kapitel 3a nicht ausdrücklich Anderes vorgesehen wird.

2.5 Artikel 10a Lage innere Sicherheit

Die Bestimmung regelt eine Aufgabe, die bereits von den Sicherheitsorganen des Bundes wahrgenommen wird (vgl. die Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement; SR 172.213.1, insbesondere Artikel 9 Absatz 2 Buchstabe a Ziffer 2).

Absatz 1
Das Bundesamt für Polizei ist verantwortlich für die ständige Lagebearbeitung im Bereich der inneren Sicherheit. Dazu führt es das Bundeslagezentrum, das die relevante Lage aus den Teilbereichen der inneren Sicherheit (Kantone, andere Bundesstellen) integriert. Das Bundeslagezentrum wirkt zudem bei besonderen Ereignissen (z.B. Grossanlässen) massgeblich an der Führung des nationalen Nachrichtenverbundes mit. Die Aufgaben bedingen einen steten Nachrichtenfluss, den es zu regeln gilt.

Absatz 2
Zur Verbreitung der Lageinformationen nutzt das Bundeslagezentrum u.a. eine Elektronische Lagedarstellung (ELD). Bei diesem elektronischen Informationssystem handelt es sich nicht um eine Datensammlung nach Datenschutzgesetz; systematische Bearbeitung von Personendaten findet keine statt. Vielmehr handelt es sich um ein Lageinformationssystem, in dem von berechtigten Stellen aktualisierte Informationen zur Lage der inneren Sicherheit abgerufen werden können. Im Ereignisfall (z.B. Nachrichtenverbund bei einer Grossveranstaltung, Terroranschlag) werden über die ELD zusätzlich ereignisbezogene Lageinformationen verbreitet.

Es besteht keine technische Verbindung zwischen dem Staatsschutz-Informations-System (ISIS) und der ELD. Bei öffentlich bekannten Personendaten handelt es sich um Daten, welche bereits durch die Medien bekannt gemacht wurden. Die übrigen Personendaten stehen untrennbar mit einem lagerelevanten Ereignis in Zusammenhang. Die Empfänger sind gemäss BWIS berechtigt, an diese Art von Informationen zu gelangen.

Absatz 3
Zugang zur periodischen Lagedarstellung der ELD erhalten jene Stellen, welche die dort abrufbaren Informationen in Übereinstimmung mit Artikel 17 (Weitergabe von Personendaten) zur Erfüllung ihrer Aufgaben benötigen. Bei zeitlich nur befristet abrufbaren Inhalten (ereignisbezogene Lagedarstellung) sowie bei Inhalten ohne besonders schützenswerte Personendaten regelt das Bundesamt den Zugang.

Absatz 4
Absatz 4 schliesst eine heute bestehende Lücke, indem beschränkt auf die ereignisbezogene Lagedarstellung und nur für eine bestimmte Zeit die Datenweitergabe an private Stellen ermöglicht wird (z.B. an im Rahmen eines Grossanlasses tätige private Sicherheitsfirmen). Entscheidend ist, dass die Datenweitergabe für die innere oder äussere Sicherheit der Schweiz nötig ist.

2.6 Artikel 13, Titel, Absätze 3 und 4 Allgemeine Auskunftspflicht der Behörden

Die Einführung von Artikel 13a bedingt eine Anpassung von Artikel 13, damit der Unterschied zwischen den beiden Formen der Auskunftspflicht besser erkennbar wird.

Titel
Der Titel von Artikel 13 wird so geändert, dass er mit dem Wort „Allgemeine“ zum Ausdruck bringt, dass diese Pflichten für den gesamten Aufgabenbereich des BWIS gelten.

Absatz 3
Da Erkenntnisse über eine Bedrohung durch Terrorismus, verbotenen politischen oder militärischen Nachrichtendienst, verbotenen Handel mit Waffen, radioaktiven Materialien oder durch verbotenen Technologietransfer dauerhaft mitzuteilen sind, ist die Delegation an den Bundesrat auf die verbleibenden Bereiche zu beschränken. Es sind dies gewalttätiger Extremismus und verbotener wirtschaftlicher Nachrichtendienst.

Absatz 4
Die in diesem Absatz bisher enthaltene Regelung wird aufgehoben und neu als eigenständiger Artikel gegliedert (vgl. Artikel 13b). Die neue Regelung gilt für allfällige Meinungsverschiedenheiten zwischen allen zur Auskunft verpflichteten Behörden, und zwar sowohl nach Artikel 13, als auch nach Artikel 13a. Abgeändert werden muss die Bestimmung auch, weil sich die Auskunftspflicht künftig nicht mehr auf Straf- und Verwaltungsbehörden beschränkt.

2.7 Art.13a Besondere Auskunftspflicht der Behörden

Die Abstimmung des Erlassentwurfes mit der vom Parlament verabschiedeten, noch nicht in Kraft gesetzten Teilrevision des BWIS in Bezug auf Gewaltpropaganda und Gewalt bei Sportveranstaltungen (Änderung vom 24. März 2006; sog. BWIS I) wird nach durchgeführtem Vernehmlassungsverfahren erfolgen.

Wie bereits erwähnt wird mit dieser Bestimmung eine neue Form der Auskunftspflicht eingeführt. Bezogen auf Artikel 13 handelt es sich um eine Spezialnorm. Einerseits beschränkt sie sich auf einen Teilbereich des gesetzlichen Aufgabenbereichs.

Anderseits geht sie weiter, indem sie für alle Behörden des Bundes, der Kantone und für Organisationen, die öffentliche Aufgaben wahrnehmen, Geltung beansprucht.

Absatz 1
Dieser Absatz legt eine Auskunftspflicht für bestimmte Gefährdungen fest (vgl. Buchstaben a bis c). Es geht dabei um Gefährdungen, die aufgrund ihres Potenzials die Grundwerte der Schweiz bedrohen können. Als solches richten sie sich gegen parlamentarische, richterliche oder Regierungsinstitutionen und stellen die Existenz oder das richtige Funktionieren der Schweiz in Frage. Werden Bürgerinnen und Bürger bei der Ausübung ihrer Volksrechte behindert oder eingeschüchtert, fördert dies ein zunehmendes Gefühl der Unsicherheit und der Staat läuft Gefahr, dass sein demokratisches System unterminiert wird. Bedrohungen der geschilderten Art kennzeichnen Terrorismus, verbotenen politischen und militärischen Nachrichtendienst und den verbotenen Handel mit Waffen oder radioaktiven Materialien sowie verbotenen Technologietransfer.

Die Bestimmung verpflichtet grundsätzlich alle Behörden und Verwaltungseinheiten des Bundes und der Kantone zur Auskunft. Zu den Verwaltungseinheiten des Bundes zählt zum Beispiel auch die Meldestelle für Geldwäscherei (MROS). Zu den Verwaltungseinheiten der Kantone gehören auch diejenigen der Gemeinden; sie sind vom Begriff « Kanton » miterfasst. Organisationen, die öffentliche Aufgaben wahrnehmen, werden ebenfalls zur Auskunft verpflichtet. Gemäss Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010) handelt es sich dabei um mit Verwaltungsaufgaben betraute Organisationen des öffentlichen oder privaten Rechts, die nicht der Bundesverwaltung angehören. Eine Auflistung der betroffenen Organisationen im Gesetz selber ist aus praktischen Gründen nicht möglich. Zudem wäre eine solche Auflistung in einem Gesetz zu einschränkend, weil gegebenenfalls den rasch ändernden Gegebenheiten nicht rechtzeitig Rechnung getragen werden könnte. Deshalb soll von einer Auflistung im Gesetz abgesehen und stattdessen für die Bezeichnung der Organisationen, die der Auskunftspflicht unterstehen, eine Delegation an den Bundesrat vorgesehen werden (vgl. Absatz 2).

Mit der Formulierung „im Einzelfall“ soll verdeutlicht werden, dass die zur Auskunft verpflichteten Behörden zwar dauerhaft, aber nur bezogen auf bestimmte, konkrete Einzelfälle und erst auf entsprechendes Auskunftsersuchen des Bundesamtes oder in seinem Auftrag handelnder kantonaler Sicherheitsorgane hin Auskunft zu erteilen haben.

Die bei den Behörden und Organisationen eingeholten Auskünfte richten sich an das Bundesamt; es ist der Empfänger. Die von den Kantonen mit Sicherheitsaufgaben betrauten Behörden können im Auftrag des Bundes tätig werden und unmittelbar bei den auskunftspflichtigen Behörden und Organisationen Auskünfte einholen, um sie dem Bundesamt zur Verfügung zu stellen. Dieses Vorgehen ist mit dem im Gesetz vorgesehenen System kohärent (vgl. Artikel 7 Absatz 1, Artikel 13 Absatz 1, Artikel 14 Absatz 1). Kommt es hinsichtlich der Auskunftspflicht zu einer Meinungsverschiedenheit, besteht diese zwischen der auskunftsverweigernden Behörde oder Organisation und dem Bundesamt, nicht aber mit der kantonalen Behörde, die im Auftrag des Bundesamtes die umstrittene Auskunft einholen wollte.

Der Sicherheit von Experten des Schweizerischen Expertenpools für zivile Friedensförderung und von Mitarbeitern, die an humanitäre oder im Menschenrechtsbereich tätige Organisationen zur Verfügung gestellt wurden, ist während im Ausland laufender Missionen besondere Achtung zu schenken. Auch gilt es allfälligen Vertraulichkeitsklauseln, speziellen Verhaltenscodices oder Standing operating Procedures (SOP) in geeigneter Form Rechnung zu tragen. Massgebend sind die jeweiligen Umstände des Einzelfalles.

Absatz 2
Aus Gründen der Rechtsstaatlichkeit dürfen die Sicherheitsorgane nicht alleine über die Auskunftspflicht einer Organisation entscheiden. Deshalb soll der Bundesrat die verpflichteten Organisationen auf dem Verordnungsweg abschliessend bezeichnen.

Absatz 3
Die in Absatz 1 und 2 genannten Stellen sind auch ermächtigt, den mit Staatsschutz befassten Behörden von Bund und Kantonen von sich aus Sachverhalte zu melden, von denen sie annehmen, dass eine Verbindung zu Terrorismus, verbotenem politischen oder militärischen Nachrichtendienst oder verbotenem Handel mit Waffen oder radioaktiven Materialien oder verbotenem Technologietransfer bestehen könnte. Die in Absatz 1 und 2 genannten Stellen sollen somit vor dem Vorwurf bewahrt werden, eine Amtsgeheimnisverletzung zu begehen. So könnte beispielsweise die MROS (vgl. obige Erläuterungen zu Absatz 1) den Sicherheitsorganen künftig unaufgefordert Informationen zur Verfügung stellen. Es besteht indessen keine Pflicht für ein systematisches Meldewesen.

Öffentliches Interesse und Verhältnismässigkeit
Mit dem neuen Artikel 13a soll die Bestimmung des heutigen Artikels 13 Absatz 3 auf Gesetzesstufe nachvollzogen werden. Es betrifft dies die Möglichkeit des Bundesrates, für begrenzte Zeit andere als die in Artikel 13 Absatz 1 aufgeführten Behörden der Auskunftspflicht zu unterstellen. Der Bundesrat machte davon Gebrauch, indem er die Verordnung vom 7. November 2001 betreffend die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit erliess. Nach zweimaliger Verlängerung gilt diese Verordnung nun noch bis zum 31. Dezember 2008 (vgl. AS 2005 5423).

Seit dem Erlass der Verordnung hat sich die Bedrohungslage der Schweiz im Bereich der terroristischen Bedrohung nicht grundlegend geändert. Die heutige Beurteilung lautet wie bisher, dass die Schweiz zwar nicht ein direktes und primäres Ziel des Terrorismus ist. Die allgemeine Gefahr für terroristische Aktionen hingegen bleibt weltweit gross, wovon auch die Schweiz – wie andere Länder - betroffen ist. Der Mittelmeerraum und Kontinentaleuropa sind nicht länger nur Ruhe- oder Vorbereitungsraum. Alles in allem ist davon auszugehen, dass Terrororganisationen bereit sind, bei sich bietender Gelegenheit mit terroristischen Anschlägen gegen westliche Interessen vorzugehen. Es ist mit einer langdauernden Auseinandersetzung zu rechnen; ein Ende der Bedrohungslage ist zum heutigen Zeitpunkt nicht absehbar.

Der Bundesrat beauftragte das EJPD im Dezember 2002, die Auskunfts- und Meldeverordnung auf ihre Wirksamkeit zu überprüfen und ihm Bericht zu erstatten. In der Folge wurde bei den Polizeikorps der Kantone und bei denjenigen der Städte

Zürich und Bern eine Umfrage durchgeführt. Dabei wurde das Schwergewicht nicht auf das Meldeaufkommen als solches (Quantität), sondern auf den inhaltlichen Wert (Qualität) der Meldungen gelegt (somit Qualität vor Quantität).

Zur Evaluation wurde ursprünglich beabsichtigt, die in einem Zusammenhang mit den erweiterten Befugnissen stehenden Meldungen im Staatsschutzinformationssystem ISIS speziell zu kennzeichnen. Dieses Unterfangen stellte sich jedoch als (viel) zu aufwändig heraus, so dass darauf verzichtet werden musste. Zum anderen erwies es sich, dass mit der blossen Markierung von Meldungen die Auswirkungen der Auskunfts- und Meldeverordnung auf kantonaler Ebene gar nicht oder bloss unzureichend erfasst wurden. Dies namentlich in denjenigen Fällen, in denen auf kantonaler Ebene Meldungen dank der erweiterten Kompetenzen mit entsprechend kleinerem Aufwand abgeklärt werden konnten, ohne dass eine spezielle Meldung an den DAP erfolgte.

Weiter wurde festgestellt, dass die Auskunfts- und Meldeverordnung zwar auf polizeilicher Seite sehr wohl, nicht jedoch auf Seiten der zur Auskunft berechtigten oder verpflichteten Personen ausreichend bekannt war. Diesem Umstand wurde anlässlich der letzten Verlängerung mit einem entsprechend breit gestreuten Kreisschreiben Rechnung getragen.

Insgesamt ergab sich eine zahlenmässig eher geringe, inhaltlich jedoch deutliche Verbesserung des Meldeaufkommens. Bisweilen wurde die blosse Existenz des entsprechenden Rechts bzw. der entsprechenden Pflicht als wichtiger als deren praktischer Nutzen beurteilt. Trotzdem lehnten die kantonalen Vollzugsorgane eine Aufhebung der Bestimmung entschieden ab. Die blosse Existenz der Verordnung wird als wichtig eingestuft. Ihre konkreten Wirkungen sind jedoch schwierig detailliert nachweisbar, weil nur ein sehr beschränktes Meldeaufkommen ausschliesslich auf die erweiterten Befugnisse zurückgeführt werden kann. Im Gegenzug hat die Verordnung kaum Kosten verursacht.

Zusammenfassend erwies sich die Verordnung sowohl innen-, wie auch aussenpolitisch von nicht zu unterschätzender Bedeutung (innenpolitisch: Gradmesser für den Willen des Bundesrates zum Kampf gegen den Terrorismus; aussenpolitisch: Signal für die Bereitschaft der Schweiz, ihre Rolle im internationalen Staatenverbund zur Bekämpfung des Terrorismus wahrzunehmen). Mit anderen Worten besteht an ihrer Weiterführung bzw. Überführung in das « ordentliche » Recht ein gewichtiges öffentliches Interesse.

Das zahlenmässig geringe, qualitativ aber hoch stehende Meldeaufkommen belegt die Verhältnismässigkeit der Massnahme.

2.8 Artikel 13b Streitigkeiten über die Auskunftspflicht

Der Anwendungsbereich von Artikel 13b ist dann gegeben, wenn das Bundesamt oder ein in seinem Auftrag tätiges kantonales Sicherheitsorgan gestützt auf Artikel 13 oder 13a eine Auskunft verlangt, die angefragte Stelle indessen nicht bereit ist, diese zu erteilen.

Absatz 1
Sind lediglich Verwaltungseinheiten der zentralen Bundesverwaltung (vgl. Artikel 7 RVOV, SR 172.010.1) hinsichtlich der Auskunftspflicht geteilter Meinung, entscheidet

die gemeinsame Aufsichtsbehörde, das heisst der Vorsteher oder die Vorsteherin des antragstellenden Departements oder der Bundesrat (vgl. Artikel 9 Absatz 3, Bundesgesetz über das Verwaltungsverfahren, SR 172.021). Käme es beispielsweise hinsichtlich einer Auskunft, die das Bundesamt für Polizei vom Bundesamt für Migration verlangt, zu Meinungsverschiedenheiten, so würde der Vorsteher oder die Vorsteherin des Eidgenössischen Justiz- und Polizeidepartements entscheiden.

Absatz 2
In allen übrigen Fällen kann das Bundesamt an das Bundesverwaltungsgericht gelangen und um einen abschliessenden Entscheid ersuchen (vgl. Artikel 83 Buchstaben a des Bundesgesetzes vom 17. Juni 2005 über das Bundesverwaltungsgericht[3]). Dieser Weg steht dem Bundesamt auch offen, wenn ein kantonales Sicherheitsorgan um die verweigerte Auskunft ersucht hat. Weil das kantonale Sicherheitsorgan im Auftrag des Bundes handelt, ist es folgerichtig, dass nicht das kantonale Sicherheitsorgan, sondern einzig das Bundesamt an das Bundesverwaltungsgericht gelangen kann.

Das Verfahren vor dem Bundesverwaltungsgericht löst das bisherige Verfahren vor dem Bundesstrafgericht nach dem heutigen Artikel 13 Absatz 4 ab; die Klärung anderer Streitigkeiten über den Anwendungsbereich des BWIS soll nach dem neuen Artikel 29a ebenfalls dem Bundesverwaltungsgericht obliegen.

Streitigkeiten über die Auskunftspflicht können sich mit eidgenössischen oder kantonalen Behörden, gleich wie mit Organisationen, die öffentliche Aufgaben wahrnehmen oder mit Stellen ausserhalb der dezentralen Bundesverwaltung (vgl. Artikel 8 RVOV, z.B. Schweizerische Bundesanwaltschaft) ergeben.

2.9 Artikel 13*c* Auskunftspflicht gewerblicher Transporteure

Die neu eingeführte Auskunftspflicht gleicht derjenigen nach Artikel 13a. Sie zielt indessen nicht auf Behörden oder auf Organisationen ab, die eine öffentliche Aufgabe erfüllen, sondern richtet sich an gewerbliche Transporteure, die in diesem Bereich Leistungen erbringen. Gleich wie die Auskunftspflicht nach Artikel 13a knüpft die Auskunftspflicht gewerblicher Transporteure an bestimmte Bedrohungsformen an (Terrorismus, verbotener politischer und militärischer Nachrichtendienst, verbotener Handel mit Waffen oder radioaktiven Materialien sowie verbotener Technologietransfer).

Die Bestimmung gilt beispielsweise für Taxiunternehmen, Flug- und Eisenbahngesellschaften, Autovermietungen, Strassentransporteure usw.

Die Transporteure sind gehalten, Auskunft über bereits vorhandene, von ihnen für ihre eigenen Zwecke erhobene Daten zu erteilen. Artikel 13c verpflichtet sie somit nicht zur Erhebung zusätzlicher Daten. Da die Auskunftserteilung über ohnehin bereits vorhandenes Datenmaterial für die Transporteure keinen nennenswerten Mehraufwand verursacht, ist keine spezielle Entschädigung durch die Sicherheitsorgane vorgesehen; die Auskunft ist unentgeltlich zu erbringen.

[3] BBl 2005 4093. Dieses Gesetz wird voraussichtlich am 1. Januar 2007 rechtskräftig.

Mit der Formulierung „im Einzelfall“ wird verdeutlicht, dass nur dann eine Auskunftspflicht besteht, wenn das Bundesamt oder ein in seinem Auftrag handelndes kantonales Sicherheitsorgan in einem konkreten Einzelfall mit einem Auskunftsbegehren an den Transporteur gelangt.

Öffentliches Interesse und Verhältnismässigkeit
Nach Artikel 14 Absatz 2 Buchstabe b BWIS dürfen die Sicherheitsorgane für die Erfüllung ihrer Aufgaben Auskünfte einholen. Gelangen sie dafür an private Personen (seien es natürliche oder juristische), so verweigern diese oft unter Hinweis auf die Datenschutzgesetzgebung die Auskunft. Um im Bereich des für die Sicherheitsorgane besonders wichtigen gewerblichen Transportgewerbes solches zu verhindern, soll eine Auskunftspflicht für gewerbliche Transporteure eingeführt werden. Mit der Auskunftspflicht wird einerseits in die Berufssphäre des Transporteurs und andererseits in die Privatsphäre der so beobachteten Person eingegriffen. Es gilt deshalb zu prüfen, ob der Eingriff in Bezug auf das zur Diskussion stehende öffentliche Interesse verhältnismässig ist. Zu betonen ist, dass Erkenntnisse von privaten Transporteuren bei der Beurteilung einer potenziellen Gefährdung von ausschlaggebender Bedeutung sein können. Bewegungen bestimmter Personen oder Güter, oder Erkenntnisse über die Häufigkeit solcher Bewegungen, erlauben oftmals erst, bestimmte konkrete Hinweise auf ihre Richtigkeit zu prüfen. Es dürfte unbestritten sein, dass der Zugang zu dieser Art von Informationen ein ebenso geeignetes wie auch notwendiges Mittel ist, damit das Bundesamt die ihm übertragenen präventive Gefahrenabwehr erfolgreich wahrnehmen kann.

Auch wenn die Verhältnismässigkeit rein abstrakt schwer zu beurteilen ist, gilt es folgende Gesichtspunkte zu berücksichtigen: Der Transporteur ist nicht zur aktiven Beschaffung von Information verpflichtet und nur gehalten, Auskunft über ihm bereits bekannte Informationen zu erteilen. Die Auskunftspflicht ist deshalb nicht a priori ein unverhältnismässiger Eingriff in seine Berufssphäre. Auch kann der Transporteur kein besonders schützenswertes Berufsgeheimnis für sich beanspruchen. Seine Kundinnen und Kunden können sich deshalb auch nicht auf ein besonderes, dem Transportvertrag innewohnendes spezielles Vertrauensverhältnis berufen.

Stammen die fraglichen Daten aus der Beobachtung an einem allgemein zugänglichen Ort, kann der Eingriff in die Privatsphäre angesichts des zu schützenden öffentlichen Interesses nicht als unverhältnismässig bezeichnet werden. In der Praxis wird aber das zu schützende öffentliche Interesse gegen das ebenfalls schützenswerte persönliche Interesse im konkreten Einzelfall abzuwägen sein.

2.10 Artikel 13d Berufsgeheimnis
Bestimmte Berufe können »nur dann richtig und einwandfrei ausgeübt werden, ... wenn das Publikum auf Grund einer unbedingten Garantie der Verschwiegenheit das unentbehrliche Vertrauen zum Inhaber des Berufes hat. « (BGE 84 IV 108). Diese Voraussetzung wird zum einen durch die Strafbarkeit von Verletzungen eines Berufsgeheimnisses (beispielsweise. Art. 321 des Strafgesetzbuchs, SR 311.0; Art. 35 des Bundesgesetzes vom 15. Juni 1992 über den Datenschutz, SR 235.1), zum andern durch die Einräumung des Rechts, auch gegenüber Behörden dem Berufsgeheimnis unterliegende Auskünfte zu verweigern, sichergestellt. Dieses Recht dient somit dem Schutz eines besonderen Vertrauensverhältnisses, welches nicht nur in gerichtlichen Verfahren, sondern immer dann zu beachten ist, wenn

Private gegenüber Behörden zur Auskunft verpflichtet werden. Entsprechend ist vorgesehen, dass Berufsgeheimnisträgern gegenüber einem Auskunftsbegehren des Bundesamtes das gleiche Recht zur Auskunftsverweigerung zukommt, wie es ihnen in einem vom Bund geführten Strafverfahren zustehen würde. Vom Auskunftsverweigerungsrecht nicht erfasst sind dagegen blosse, auf Vertrag beruhende Geheimhaltungspflichten, selbst wenn diese ihre sachliche Grundlage auf der beruflichen Tätigkeit der zur Geheimhaltung verpflichteten Person haben.

2.11 Artikel 14, Absatz 3
Der Artikel 14 BWIS listet die Mittel abschliessend auf, derer sich die Sicherheitsorgane zur Erfüllung ihrer Aufgaben derzeit bedienen dürfen. Der Einsatz dieser Mittel hat keine schwerwiegende Einschränkung der Grundrechte zur Folge. Während diese bisherigen Mittel zur Informationsbeschaffung auch weiterhin von Bedeutung sind und von den Sicherheitsorganen überwiegend angewendet werden, kann die in Kapitel 3a genannte Informationsbeschaffung mit besonderen Mitteln nur unter bestimmten Umständen und subsidiär eingesetzt werden.

Absatz 3
Im geltenden Gesetz ist diese Bestimmung von grosser Bedeutung. Sie untersagt es den Sicherheitsorganen im präventiven Bereich generell, strafprozessuale Zwangsmassnahmen anzuwenden oder in Privaträumen Vorgänge zu beobachten. Mit der Revision soll der präventive Einsatz von Zwangsmassnahmen – die Informationsbeschaffung mit besonderen Mitteln – eingeführt werden, die unter restriktiven Voraussetzungen eingesetzt werden dürfen. Galt bisher ein generelles Verbot, führt die Revision neu ein System der Ausnahmeregelung mit Bewilligungspflicht ein. Die Bestimmung in Absatz 3 ist damit hinfällig und wird aufgehoben, auch wenn es sich bei den besonderen neuen Mitteln nicht um Zwangsmittel im strafprozessualen Sinn, sondern um nachrichtendienstliche Informationsbeschaffungsmittel handelt.

Die Informationsbeschaffung mit besonderen Mitteln darf nur eingesetzt werden, wenn die Bedingungen von Artikel 18a und den folgenden Artikeln gegeben sind. Konkret bedeutet dies vor allem, dass besondere Mittel nur in den Tätigkeitsbereichen eingesetzt werden dürfen, für die sie vorgesehen sind: Terrorismus, verbotener politischer und militärischer Nachrichtendienst und verbotener Handel mit Waffen und radioaktiven Materialien sowie verbotener Technologietransfer. Hingegen ist kein Einsatz möglich, um Informationen bezüglich eine Gefährdung durch gewalttätigen Extremismus oder wirtschaftlichen Nachrichtendienst zu beschaffen (vgl. Kommentar zu Artikel 13 Absatz 3). Die besonderen Mittel der Informationsbeschaffung dürfen ferner nicht eingesetzt werden, wenn die Gefährdung nicht erheblich oder ihre Plausibilität nicht hinreichend konkret ist oder auf Tatsachen beruht, die nicht präzise genug oder nicht genügend aktuell sind.

2.12 Artikel 14a Funkaufklärung
Die Sicherheitsorgane des Bundes befassen sich seit Jahrzehnten mit der Aufklärung von Funkausstrahlungen ausländischer Nachrichtendienste, welche mit nachrichtendienstlichen Bestrebungen gegen die Schweiz zusammenhängen könnten. Diese Ausstrahlungen finden zu einem grossen Teil nach wie vor im Spektrum der Kurzwelle statt und sind nicht besonders gegen den Empfang durch Dritte geschützt (vgl. hierzu auch Staatsschutzbericht 2000, S. 147 f.). Zum Zeitpunkt des Erlasses

des BWIS wurde diese Tätigkeit deshalb unter die Beschaffung im Rahmen der Beobachtung von Vorgängen an öffentlichen und allgemein zugänglichen Orten gezählt (Artikel 14 Absatz 2 Buchstaben f. BWIS).

In den letzten Jahren hat das VBS mit dem Projekt ONYX Kapazitäten zur Aufklärung von Fernmeldeverkehr aufgebaut, der international via Satelliten übertragen wird. Dabei werden Ausstrahlungen der Satelliten auf die Erde erfasst und ausgewertet, die dort normalerweise auch von den kommerziellen Fernmeldedienstleistern erfasst und weitergeleitet werden. Seit April 2001 nimmt der DAP im Rahmen eines Testbetriebes an der Nutzung des Systems ONYX teil. Eine Rechtsgrundlage wurde hierzu in Artikel 9a VWIS geschaffen. Die Überführung dieser Bestimmung in das Gesetz (BWIS) soll mit der vorliegenden Revision erfolgen. Damit wird auch eine Forderung der Geschäftsprüfungsdelegation erfüllt, welche eine ausdrückliche gesetzliche Grundlage für die Nutzung von ONYX verlangt. Für die Nutzung von ONYX durch die Nachrichtendienste im VBS erfolgt parallel eine Änderung des Militärgesetzes (vgl. Änderung bisherigen Rechts, Ziffer 3, Artikel 99 Abs. 1 und 1^{bis} und Artikel 99a MG).

Der neue Artikel 14 a BWIS entspricht weitgehend der heutigen Regelung der VWIS. Er wurde mit der Möglichkeit zur allfälligen Überwachung von Inlandszielen ergänzt, die unter den Bedingungen und dem Verfahren nach den neuen Artikeln 18d ff. erlaubt ist. Es wäre widersprüchlich, wenn eine Person, deren Fernmeldeanschlüsse im Inland überwacht werden dürfen, für diese Zeit nicht auch als Aufklärungsziel der Funkaufklärung definiert werden könnte.

Absatz 1
Dieser Absatz ist die Grundlage dafür, dass fedpol mit dem Mittel der Funkaufklärung Ziele im Ausland erfassen und die Erkenntnisse auswerten kann, und er definiert den Begriff der Funkaufklärung. Die Definition umfasst alle Arten von elektromagnetischen Ausstrahlungen aus dem Ausland. Eine Beschränkung auf bestimmte technische Anwendungen wie Kurzwelle oder ONYX wäre angesichts der rasanten Entwicklung der Telekommunikationstechnik in diesen Bereichen weder sachlich noch rechtlich sinnvoll.

Absatz 2
Der erste Satz bezieht sich auf die Beschaffung technischer Informationen über Ausstrahlungen aus der Schweiz wie verwendete Frequenzen, Sendestärken oder Sendezeiten. Er betrifft somit Daten die nicht unter das Fernmeldegeheimnis im Sinne von Artikel 13 Absatz 1 BV und des Fernmeldegesetzes fallen. Dient die Funkaufklärung aber dazu, Mitteilungen zu überwachen, die unter das Fernmeldegeheimnis fallen, (vgl. über das Mobiltelefon hergestellte Verbindungen), verweist der zweite Satz im zweiten Abschnitt klar und deutlich darauf, dass diese Form der Aufklärung wie die Überwachung des Post- oder Fernmeldeverkehrs ein besonderes Mittel der Informationsbeschaffung darstellt und deshalb die Bestimmungen unter Kapitel 3a zur Anwendung kommen (vgl. Artikel 18a und folgende Artikel, insbesondere Artikel 18k). Damit sind auch Fälle klar den strengeren Regelungen unterworfen, in welchen die technische Unterstützung von Fernmeldedienstleistern für die Überwachung nicht beansprucht wird.

Absatz 3
Die heutige Praxis der technischen Kooperation der Bundesstellen ist in dieser Bestimmung verankert: Die Bestimmung ermächtigt das Bundesamt, im Zuge der Funkaufklärung mit anderen Stellen des Bundes und der Kantone zusammenzuarbeiten. Fedpol betreibt nur in geringem Umfang eigene Anlagen für die Erfassung von Kurzwellenfunk und ist im Wesentlichen selbständiger Auftraggeber der Abteilung Elektronische Kriegführung im VBS. Hingegen ist, nach dieser Bestimmung, ein Anschluss an ein ausländisches Funküberwachungssystem (beispielsweise ECHELON) weiterhin nicht zulässig.

Absatz 4
Dieser Absatz stellt sicher, dass im Bereich der ständigen Funkaufklärung in jedem Fall die Kontrollinstrumente gemäss Artikel 99 ff. des Militärgesetzes zur Anwendung kommen (vgl. Änderung bisherigen Rechts, Ziffer 3, Militärgesetz, insbesondere Artikel 99a). Damit keine Diskrepanz zur vom Umfang her weit bedeutenderen Funkaufklärung zu Gunsten der Nachrichtendienste des VBS entsteht, soll die Kontrolle über die Aufklärung von reinen Auslandszielen weiterhin bei derselben Kontrollinstanz (heute unabhängige Kontrollinstanz UKI, nach vorliegendem Entwurf die „unabhängige Aufsichtsbehörde“) erfolgen. Bei allfälligen Inlandszielen muss jedoch das Verfahren gemäss Artikel 18d und 18e (vgl. nachfolgend) durchgeführt werden, soweit die Massnahme oder die Funkaufklärung Fernmeldeverkehr betrifft, der unter das Fernmeldegeheimnis fällt.

Öffentliches Interesse und Verhältnismässigkeit
Die Funkaufklärung ist ein Mittel zur Informationsbeschaffung aus Quellen, die grundsätzlich öffentlich zugänglich sind. Der Einsatz dieses Mittels stellt deshalb an sich keinen erheblichen Eingriff in die Privatsphäre dar und insbesondere auch keine erhebliche Verletzung des Fernmeldegeheimnisses. Bestimmte Arten des Funkverkehrs, die mithilfe der Funkaufklärung überwacht werden können, fallen aber unter das Fernmeldegeheimnis. Hier kann die Funkaufklärung erheblich in die Privatsphäre eingreifen. In solchen Fällen kommen die Bestimmungen über die besonderen Mittel der Informationsbeschaffung zur Anwendung, insbesondere jene des Artikels 18k hinsichtlich der Überwachung des Post- oder Fernmeldeverkehrs. Weitere diesbezügliche Erwägungen finden sich in den Erläuterungen zu diesem Artikel.

2.13 Artikel 14b Informantinnen und Informanten

Die Sicherheitsorgane sind zur Wahrnehmung ihrer Aufgaben auf Mitteilungen von Personen angewiesen, die Zugang zu relevanten Informationen haben. In Übereinstimmung mit dem in der Bundesverfassung verankerten Legalitätsprinzip müssen alle wichtigen rechtsetzenden Bestimmungen in einem formellen Gesetz erlassen werden (vgl. Artikel 164 Absatz 1 BV). Während das heutige BWIS den Einsatz von Informantinnen oder Informanten dem Prinzip nach impliziert, finden sich keine spezifischen Bestimmungen über deren Einsatz, deren Rechte, Pflichten oder über Leistungen seitens des Staats (vgl. insbesondere Artikel 14 Absatz 2 Buchstaben b und d zum Einholen von Auskünften und Entgegennehmen von Meldungen). Diese rudimentäre Rechtslage muss neu präzisiert werden.

Absatz 1
Die Bestimmung in diesem Absatz befugt das Bundesamt ausdrücklich dazu, Informantinnen und Informanten einzusetzen, und definiert diese. Dabei handelt es

sich um Personen, die freiwillig mit Sicherheitsorganen zusammenzuarbeiten, ohne dass jedoch ein Arbeitsvertrag im Sinne von Artikel 319 des Obligationenrechts (OR; SR 220) entsteht. Der Umstand, dass diesen Personen fallweise eine Prämie entrichtet werden kann oder dass ihnen ihre Auslagen erstattet werden (vgl. Absatz 2), ist kein Grund dafür, dieses Verhältnis als Arbeitsvertrag zu qualifizieren. Für einen Arbeitsvertrag im Sinne von Artikel 319 des Obligationenrechts bedürfte es weiterer konstituierender Elemente, so beispielsweise eines formalrechtlichen Unterordnungsverhältnisses, wodurch die Informantin oder der Informant personalrechtlich, organisatorisch und zeitlich vom Bundesamt abhängig wäre. Dies ist in der Praxis klar nicht der Fall.

Absatz 2
Damit Informantinnen oder Informanten, die die Staatsschutzorgane mehr oder weniger regelmässig mit Informationen versorgen, durch ihre Tätigkeit keine finanziellen Einbussen erleiden, werden ihnen ihre Auslagen zurückerstattet. Es handelt sich bei diesen Entschädigungen nicht um steuerbares Einkommen oder Lohn im Sinne der AHV-Gesetzgebung. Unkosten sind Auslagen, die der Informantin und dem Informanten bei der Ausführung ihrer Tätigkeit entsteht.

Zudem können Informantinnen und Informanten für besonders wichtige Informationen fallweise Prämien erhalten. Die Prämien bewegen sich in der schon heute geübten Praxis auf einem bescheidenen Niveau von höchstens wenigen Tausend Franken jährlich und erreichen die Höhe eines existenzerhaltenden Einkommens bei weitem nicht. Damit kein falsch verstandener Erfolgsdruck entsteht, soll der finanzielle Anreiz für die Tätigkeit einer Informantin oder eines Informanten nicht ausschlaggebend sein. Prämien werden entrichtet, wenn die Person Informationen geben kann, welche die weitere Informationsbeschaffung oder die Beurteilung der Gefährdungslage wesentlich erleichtern.

Absatz 3
Das Verhältnis der Sicherheitsorgane zu Informantinnen und Informanten beruht auf gegenseitigem Vertrauen und auf der Vertraulichkeit der Beziehung nach aussen. Sie können bei den staatsschutzrelevanten Einsatzgebieten hohen Risiken ausgesetzt sein, wenn ihre Arbeit zugunsten der Sicherheitsorgane den Zielpersonen bekannt würde. Sie können deshalb weder in Personalakten des Amtes figurieren, noch können sie bei Sozialversicherungen gemeldet werden, sei es auch nur zur Feststellung, dass sie von der Versicherungspflicht befreit sind. Ihr Einsatz wird hingegen schon heute vom Eidgenössischen Justiz- und Polizeidepartement und von der Geschäftsprüfungsdelegation als ordentliche Kontrollorgane des BWIS auf Rechtmässigkeit und Zweckmässigkeit hin kontrolliert. Mit Absatz 3 soll neu klargestellt werden, dass allfällige Entschädigungen keiner Abgabepflicht unterliegen, soweit es für den Quellenschutz oder die weitere Informationsbeschaffung notwendig ist. Weder die Betroffenen noch das Gemeinwesen erleiden dadurch einen spürbaren Schaden, da es sich insgesamt um geringe Beträge handelt.

2.14 Artikel 14c Schutz von Informantinnen und Informanten

Das Ziel dieser Massnahmen ist der Schutz von Personen, die für die Beschaffung von Informationen für die Zwecke des BWIS Risiken auf sich nehmen. Darunter fallen namentlich zwei Personengruppen: Einerseits geht es um den Schutz von Personen, die von sich aus mit den Sicherheitsorganen kooperieren, und deswegen Repressalien befürchten müssen. Andererseits soll mit der Gewährung

entsprechenden Schutzes aussagewilligen Personen die Kooperation ermöglicht bzw. erleichtert werden, um so notwendige Informationen zu beschaffen. Damit würde vermieden, dass (wie dies in der Vergangenheit in der Schweiz bereits mehrfach geschah) hochkarätige aussagewillige Informanten an ausländische Nachrichtendienste, die entsprechenden Schutz gewähren können, »abgegeben« werden müssen, weil die Schweiz über keine entsprechenden Möglichkeiten verfügt.

Personen, die von sich aus mit den Sicherheitsorganen kooperieren, gehen unter Umständen erhebliche Risiken ein und müssen Nachstellungen befürchten, sei es aus ihrem persönlichen Umfeld (zum Beispiel Informantinnen und Informanten aus dem hiesigen Umfeld gewalttätiger Extremistengruppen), sei es durch fremde Staaten (beispielsweise menschliche Quellen bei Gegenoperationen, die sich zum Schein verpflichtet haben, primär aber für die Schweizer Behörden tätig sind). Die Gefährdungslage dieser Leute lässt sich mit derjenigen von verdeckten Ermittlern vergleichen, die über einen weit reichenden Schutz verfügen. Von daher rechtfertigt es sich, ja drängt sich nachgerade auf, auch für Informantinnen und Informanten Möglichkeiten zur Gewährung eines wirksamen Schutzes zu schaffen.

Die Schutzregelungen sind von der Kronzeugenregelung klar zu unterscheiden, die ursprünglich aus dem angloamerikanischen Strafprozessrecht stammt. Als Kronzeugen kommen dort Personen in Frage, die zwar grundsätzlich als mitverantwortlich für die in Frage stehende Straftat erscheinen, die jedoch unter Zusicherung der Straffreiheit, Strafreduktion oder anderer prozessualer Vorteile dafür gewonnen werden können, gegen Mitbeschuldigte als Zeugen auszusagen. Eine Expertenkommission des Bundes kam in ihrem Bericht „Vereinheitlichung des Strafprozessrechts“ zum Schluss, dass die Einführung der Kronzeugenregelung in der Schweiz auf strafprozessualer Ebene nicht angezeigt ist. Gleich verhält es sich auf präventiver Ebene. Eine Strafbefreiung im Sinne der erwähnten Kronzeugenregelung steht nicht zur Diskussion. Bei der Prävention liegt der Fokus nicht auf der Aufklärung von Straftaten, die mit besonderen Zeugenaussagen erleichtert werden soll, sondern auf dem Erhalt von Informationen, die für die Sicherheit bedeutsam sind; damit sollen Gefährdungslagen erkannt und entschärft und wenn möglich zukünftige Delikte verhindert werden.

Im Übrigen dürfte die Massnahme nur in seltenen Ausnahmefällen mit zu erwartendem hochkarätigem Informationsgewinn zum Einsatz gelangen. Zu denken ist an den Schutz von Personen, die wichtige Informationen zur Verhinderung von erheblichen sicherheitspolitischen Risiken geben können, beispielsweise über Planung oder Vorbereitung von Terroranschlägen, konkrete Spionageaktivitäten gegen die Schweiz oder Strukturen zur Beschaffung von Massenvernichtungswaffen unter Missbrauch der Schweiz. Um die mit einer Kooperation einhergehende Gefährdung zu minimieren, würden hier nach der ersten Kontaktnahme Sondierungsgespräche erfolgen und bei gegebenen Voraussetzungen eine Schutzvereinbarung mit gegenseitigen Rechten und Pflichten verhandelt. Daran würde sich die Kooperation im eigentlichen Sinne anschliessen.

Absatz 1
Mit der Bestimmung in diesem Absatz wird die rechtliche Grundlage für Massnahmen zum Schutz von Informantinnen und Informanten geschaffen. Bei den notwendigen Massnahmen, die das Bundesamt treffen muss, um Leib und Leben dieser Personen zu schützen, handelt es sich um Personenschutzmassnahmen und örtliche

Veränderungen. Unter Personenschutz sind Massnahmen zu verstehen wie der Einsatz von Leibwächtern, Schutzfahrzeugen oder –geräten oder bauliche Massnahmen. Die örtliche Veränderung kann in einem mit Zustimmung der betroffenen Person erfolgten Wechsel an einen anderen Aufenthaltsort im In- oder Ausland bestehen. Geeignete Schutzvorkehrungen zugunsten einer ins Ausland verbrachten Person bedeuten, dass eine Person, der auf Grund der Gesamtumstände trotz allem in der Schweiz kein geeigneter Schutz geboten werden kann, an einen sichereren Ort im Ausland gebracht wird. Um die damit verbundenen Umtriebe, eventuell auch einen Erwerbsausfall zu kompensieren, muss diese Massnahme mit einer befristeten finanziellen Unterstützung verbunden werden.

Das Bundesamt kann die Schutzmassnahmen selbst treffen oder sie finanzieren. In der Praxis werden nur wenige solche Massnahmen notwendig sein und sich auch umsetzen lassen. Da sich aufgrund der kleinen Grösse der Schweiz hierzulande für bestimmte Gefährdungslagen kaum umfassende Schutzmassnahmen realisieren lassen, müsste dafür ein entsprechendes Leistungspaket („package“) im Ausland eingekauft werden, womit auch die Kosten kalkulierbar sind. Denkbar ist des Weiteren auch die Gewährung von Teilschutzaspekten, beispielsweise die Zusicherung einer Aufenthaltsregelung (sei es in der Schweiz oder in einem befreundeten Drittstaat). Der zweite Satz von Artikel 1 weist ausdrücklich auf diese Möglichkeit hin.

Absatz 2
Aus denselben Überlegungen muss das Bundesamt auch Schutzvorkehrungen zugunsten von Personen treffen können, die einer Informantin oder einem Informanten nahe stehen, wenn deren Sicherheit von diesen Vorkehrungen abhängt. Mit der Kann-Formulierung wird sichergestellt, dass das Bundesamt über den notwendigen Ermessensspielraum verfügt, um von Fall zu Fall die geeigneten Massnahmen treffen zu können.

Absatz 3
Diese Bestimmung sieht als Schutzmassnahme das Ausstatten mit einer Tarnidentität vor, die im Unterschied zu den in den Absätzen 1 und 2 genannten Massnahmen erst getroffen wird, wenn das Bundesamt seine Kontakte zu einer Informantin oder einem Informanten beendet und die Informationsquelle nicht länger einsetzt. Ist die Sicherheit dieser Person wegen ihrer Zusammenarbeit mit dem Bundesamt erheblich gefährdet, kann es diese Person mit einer bleibenden Tarnidentität ausstatten, um sie zu schützen. Die Person ist in der Folge berechtigt, diese Identität nach den Instruktionen des Bundesamtes zu benutzen. Voraussetzung für eine Tarnidentität ist das Vorliegen einer positiven Stellungnahme des Bundesverwaltungsgerichts und der Ermächtigung des Departementvorstehers oder der Departementsvorsteherin (vgl. nachfolgend).

Diese Bestimmung regelt aber nicht die Informationsbeschaffung unter Verwendung einer Tarnidentität: Die Informationsbeschaffung mithilfe einer Tarnidentität darf nur unter besonderen Bedingungen und nach dem besonderen Verfahren eingesetzt werden (siehe dazu die Erläuterungen zu Artikel 14d).

Das Departement ist gemäss Artikel 27 Absatz 1bis (neu) dazu verpflichtet, den Bundesrat und die parlamentarischen Kontrollstellen regelmässig über die Zahl der

erstellten Tarnidentitäten, über den Zweck, zu dem sie erstellt worden sind, und ihren konkreten Einsatz zu unterrichten. Dies gilt auch für Tarnidentitäten nach Absatz 3.

Absatz 4
Dieser Absatz bestimmt, dass Schutzvorkehrungen im Normalfall zeitlich zu befristen sind. Das Gesetz kann die Dauer indessen nicht abschliessend festlegen, da sie den Erfordernissen des Einzelfalles angepasst werden müssen. Ausnahmsweise kann der Departementsvorsteher oder die Departementsvorsteherin von einer zeitlichen Begrenzung absehen, wenn eine Person erkennbar auf Dauer besonders stark gefährdet ist; in einem solchen Fall können die Schutzvorkehrungen unbefristet aufrechterhalten werden.

2.15 Artikel 14d Tarnidentitäten
Nachrichtendienste sind zur Wahrnehmung ihrer Aufgaben und zum Schutz ihrer Mitarbeitenden bei der Beschaffung von Informationen in bestimmten Umfeldern auf die Nutzung von Tarnungen angewiesen. Die Schaffung solcher Tarnidentitäten ist dabei immer auf Dauer angelegt und kann selten erst mit der Aufnahme eines bestimmten Falles begonnen werden. Die Regelung der Tarnidentitäten gehört deshalb nicht in den Bereich der besonderen Mittel der Informationsbeschaffung, die an sehr restriktive Voraussetzungen gebunden ist. Der strategische Nachrichtendienst SND verfügt seit 1998 auf Basis von Artikel 99 des Militärgesetzes über die Möglichkeit, seine Beschaffungsorgane mit Tarnidentitäten auszustatten (vgl. Jahresbericht 2002/2003 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation vom 23. Januar 2004; BBl 2004 1743). Die Kontrolle hierüber üben der Vorsteher des VBS und der Sicherheitsausschuss aus.

Es obliegt dem Departementsvorsteher oder der Departementsvorsteherin EJPD, das Bundesamt im Einzelfall zu ermächtigen, eine Tarnidentität zu schaffen. Vorab prüft das Bundesverwaltungsgericht (Artikel 18d), ob die Massnahme rechtsmässig ist, das heisst, ob die gesetzlichen Voraussetzungen dafür gegeben sind. Erst dann kann der Departementsvorsteher oder die Departementsvorsteherin seine bzw. ihre staatspolitische Beurteilung vornehmen und gegebenenfalls sein Einverständnis erteilen.

Theoretisch könnte die Lage entstehen, dass in gewissen Arbeitsgebieten sowohl Mitarbeitende nach BWIS als auch Beschaffer des SND, als auch verdeckte Ermittler der Kriminalpolizeien des Bundes oder der Kantone tätig sind, letztere nach Massgabe des Bundesgesetzes über die verdeckte Ermittlung (SR 312.8). Innerhalb des Bundesamtes für Polizei können solche Situationen intern durch die Amtsaufsicht der Direktion bereinigt werden. Im Verhältnis zum SND müssen allfällige Konflikte durch die vom Bundesrat am 22. Juni 2005 beschlossenen Absprachen zwischen SND und DAP vermieden werden, soweit der SND seine Legendierungen in der Schweiz einsetzt.

Absatz 1
Dieser Absatz schafft die Grundlage für den Einsatz von Tarnidentitäten zum Zweck der Informationsbeschaffung und zur Gewährleistung der Sicherheit von Beschaffungsorganen. Vorab sei darauf hingewiesen, dass die Verwendung von Tarnidentitäten sich meistens im Rahmen der allgemeinen Informationsbeschaffung bewegt, also für Massnahmen nach Artikel 14 Absatz 2 BWIS. Wenn hingegen bestimmte Massnahmen mit besonderen Mitteln der Informationsbeschaffung

durchgeführt werden sollen, welche die Verwendung einer Tarnidentität erfordern (beispielsweise eine Observation an nicht allgemein zugänglichen Orten, auch unter Verwendung einer Tarnidentität), so gelangt das Verfahren der Besonderen Informationsbeschaffung nach Artikel 18a ff. zur Anwendung. Im Übrigen wird der Personenkreis, der mit einer Tarnidentität ausgestattet werden kann, in Absatz 1 abschliessend aufgezählt:

Buchstaben a und b: Die Sicherheitsorgane gemäss BWIS sind zwar eng an die schweizerischen Polizeikräfte gebunden und können den Grossteil ihrer Beschaffungstätigkeiten offen als Polizei durchführen. Trotzdem ist es bei der Anbahnung von Kontakten zu Strukturen namentlich im Bereich des Terrorismus oder des verbotenen Nachrichtendienstes bisweilen nötig, dies unter Tarnung vornehmen zu können. Solche Massnahmen dienen nicht zuletzt auch dem Schutz der Mitarbeitenden der Sicherheitsorgane und ihrer Familien.

Buchstabe c: Auch Drittpersonen (Informantinnen und Informanten) sollen mit Legenden ausgestattet werden können, wenn dies für die Nachrichtenbeschaffung unentbehrlich ist. Zu denken ist namentlich an Personen, die sich leichter in bestimmte staatsschutzrelevante Kreise einschleusen lassen, als Mitarbeiter des Bundesamtes, und die für Ihren Schutz eine Tarnidentität benötigen. Informantinnen und Informanten werden zwar von den Führungsoffizieren der Sicherheitsorgane bezüglich der Informationsbeschaffung eng geführt, stehen aber nicht unter der direkten Dienstaufsicht der Sicherheitsorgane. Deshalb soll der Einsatz von Tarnidentitäten in diesen Fällen zeitlich und örtlich beschränkt und nur im Zusammenhang mit einer bestimmten Operation möglich sein.

Mit der Schaffung einer Tarnidentität ist auch das Recht verbunden, unter ihr Rechtsgeschäfte zu tätigen, namentlich Tarnstrukturen zu errichten. Personen mit einer Tarnidentität haben die volle Rechtspersönlichkeit und können Verträge schliessen (z.B. Anmieten von Lokalitäten und Fahrzeugen oder Fernmeldeanschlüssen, Schaffung von Tarnstrukturen wie Firmen oder andere juristische Personen).

Absatz 2
Um die Risiken besser kontrollieren zu können, die mit der Verwendung einer Tarnidentität verbunden sind, empfiehlt es sich, die Zeit zu begrenzen, während der eine Tarnidentität verwendet werden darf. Diese Vorkehrung ist besonders bei Informantinnen und Informanten angezeigt, die keine Angestellten des Bundesamtes sind und somit nicht dessen Disziplinargewalt unterstehen.

Absatz 3
Absatz 3 stellt sicher, dass eine Tarnidentität nur zu den vom BWIS verfolgten Zwecken gebraucht werden darf. Des Weiteren sei darauf hingewiesen, dass nach Artikel 27 Absatz 1^{bis} Buchstabe a des vorliegenden Entwurfs das Ausstellen und die Verwendung der Tarnidentitäten Gegenstand einer gezielten, intensiven politischen Kontrolle sein soll, in deren Rahmen das Departement den Bundesrat und die Geschäftsprüfungsdelegation jährlich zu unterrichten hat.

2.16 Artikel 15, Absatz 6
Die Bestimmung gründet in der Regelung der alten Bundespolizei, wo Repression und Prävention vereint waren. Mit der Trennung von Repression und Prävention und

deren organisatorischen Umsetzung wurde die Bestimmung obsolet. Nach heutigem Recht und Verständnis geht mit dem Informationsfluss von der Repression an die Prävention eine Zweckänderung einher; die Daten werden zu Daten präventiver Natur und sind nach dem in der Prävention anwendbaren Recht zu bearbeiten. Die Aufhebung bedeutet nicht, dass keine Daten mehr ausgetauscht werden könnten.

2.17 Artikel 16 Absatz 3, zweiter Satz
Gemäss Artikel 16 Absatz 3 Satz 1 BWIS unterstehen Daten, die von kantonalen Sicherheitsorganen nach diesem Gesetz bearbeitet werden, dem Datenschutzrecht des Bundes. Weiter hält Satz zwei fest, dass die im kantonalen Recht vorgesehenen Aufsichtsrechte gewahrt bleiben. Mit anderen Worten wird für die Bearbeitung von aus dem Aufgabenbereich des BWIS stammenden (und somit bundesrechtlichen) Daten durch kantonale Organe grundsätzlich das Datenschutzrecht des Bundes für anwendbar erklärt. Im Sinne einer Ausnahmeregelung muss das eidgenössische Recht jedoch hinter das kantonale zurücktreten, wenn und soweit das kantonale Recht eine spezielle Aufsicht vorsieht.

In der Praxis hat sich der Vorbehalt des kantonalen Aufsichtsrechts als problematisch erwiesen, weil damit einerseits eine kantonale Aufsichtsbehörde – beispielsweise eine kantonale Geschäftsprüfungskommission – Zugang zu operativen Akten des Bundes verlangen kann, und dies selbst dann, wenn die Akten auf Bundesebene klassifiziert wurden. Anderseits könnte der Wortlaut der Bestimmung zur (irrigen) Annahme verleiten, dass vom Kanton im Rahmen eines umfassenden Auftrages (z.B. Beobachtungsliste) vermeintlich „selbständig“ erhobene Daten vor deren Übermittlung an die Bundesbehörde als kantonale Daten gelten. In beiden Fällen können indessen Sicherheitsinteressen den Ausschluss jedes Einsichtsrechtes gebieten. Deshalb soll in Artikel 16 Absatz 3 BWIS neu der Bundesrat für zuständig erklärt werden, festzulegen, in welche Bundesakten die kantonalen Kontrollbehörden Einsicht nehmen können. Der Umfang des kantonalen Aufsichtsrechts wird somit vom Bundesrat festgelegt; berechtigten kantonalen Interessen kann auch inskünftig Rechnung getragen werden.

2.18 Artikel 17 Absatz 3, Buchstaben e und Absatz 7
Absatz 3 Buchstabe e
Beim sog. Clearing handelt es sich um eine traditionelle Aufgabe des DAP im Verkehr mit dem Ausland. Er führt auf Ersuchen eines ausländischen Dienstes eine Personensicherheitsprüfung über Schweizerinnen oder Schweizer oder dauerhaft in der Schweiz wohnhafte ausländische Personen durch um diesen die Mitarbeit an klassifizierten ausländischen Projekten (oder Anstellungen) zu ermöglichen. Dabei sichert der ersuchende ausländische Staat dem DAP schriftlich zu, über das Einverständnis der betroffenen Person zur Vornahme des Clearings zu verfügen.

Für die Vornahme der Clearings stützt sich der DAP seit jeher auf Artikel 17 Abs. 3 Buchstaben c BWIS. In der Vergangenheit wurde diese Rechtsgrundlage jedoch von verschiedener Seite in Frage gestellt. Deshalb soll nun eine formelle Gesetzesgrundlage für Clearings geschaffen werden. Dieser Schritt ist notwendig, damit die Stellen im Bundesamt für Polizei, welche Clearings durchführen, im Rahmen des vom Bundesamt für Justiz vorbereiteten Gesetzgebungsprojekts zur Neuregelung der Zugriffsrechte des Bundesamts für Polizei auf VOSTRA (Datenbank für Strafregisterauszüge) mitberücksichtigt werden können. Denn für den Zugriff des Bundesamts für Polizei auf VOSTRA zum Zwecke des Clearings braucht es aus

datenschutzrechtlicher Sicht zusätzlich eine klare Rechtsgrundlage in Artikel 359 ff. StGB. Die vorliegende BWIS-Änderung schafft somit lediglich die Grundlage, damit in Zukunft auch eine klare Regelung für den Zugriff auf Strafregisterdaten möglich wird. Die Strafregisterauszüge bilden für Clearings ein wichtiges Beurteilungselement. Ohne dieses würde das Clearing durch den DAP für das Ausland mit entsprechend negativen Auswirkungen auf die zu „clearende" Person an Wert verlieren. Sie würde möglicherweise auch bei positivem Ausgang des Clearings nicht mehr als genügend vertrauenswürdig gelten, um im Ausland an geheimen oder vertraulichen Projekten mitzuarbeiten.

Absatz 7
Die nachrichtendienstliche Tätigkeit beruht in erster Linie auf der Beschaffung und der Verarbeitung von Informationen. Um an Informationen zu gelangen, bedienen sich Nachrichtendienste verschiedener Beschaffungsarten. Eine davon ist die Human Intelligence (sog. HUMINT). Human Intelligence ist die Beschaffung von sensiblen Informationen durch und mit Hilfe von Menschen (sog. Quellen). Viele wichtige Informationen werden nur mitgeteilt, wenn die zuständigen Behörden verbindlich zusichern können, dass die Quelle einer Information Dritten nicht bekannt gegeben wird (sog. Quellenschutz).

Das BWIS sieht in Artikel 17 Absatz 7 ausdrücklich vor, dass im Verkehr mit dem Ausland der Quellenschutz in jedem Fall gewährleistet werden muss. In Bezug auf das Inland regelt der Bundesrat nach Artikel 17 Absatz 1 BWIS durch Verordnung, an welche Empfänger in der Schweiz, die öffentliche Aufgaben erfüllen, das Bundesamt im Einzelfall Personendaten weitergeben kann, soweit es zur Wahrung der inneren oder äusseren Sicherheit oder zur Kontrolle seiner Aufgabenerfüllung notwendig ist. Im Inlandbezug stellt sich folglich die Frage des Quellenschutzes namentlich in diesen Fällen von Informationsweitergabe.

Nach Artikel 99 Absatz 4 des am 1. Januar 2004 in Kraft getretenen Militärgesetzes (MG) geniessen Quellen des strategischen Nachrichtendienstes (SND) absoluten Schutz: „Der Quellenschutz muss in jedem Fall gewährleistet werden."

Es stellt sich deshalb die Frage, ob es sich eine unterschiedliche Behandlung der Quellen des Inland- und des Auslandnachrichtendienstes rechtfertigen lässt. Zwar gibt es Argumente für einen Beibehalt der heutigen Regelung, doch spricht mehr für eine Harmonisierung mit dem Militärgesetz. Für den Status quo kann auf die Erwägungen verwiesen werden, die den Gesetzgeber 1997 dazu führten, bei inländischen Quellen auf den absoluten Quellenschutz zu verzichten. Der Bundesrat befürchtete damals, dass sich Behörden gegenüber der Person, die Informationen mitteilt, dazu verpflichtet, die Herkunft dieser Information selbst dann nicht preiszugeben, wenn sich die Person strafbar gemacht hat. In der Botschaft zum Gesetzesentwurf schrieb der Bundesrat: »Bei Quellen im Inland kann z. B. nicht immer die strikte Vertraulichkeit zugesichert werden, zum Beispiel wenn die Gewährsperson sich selber strafbar gemacht hat. Gegenüber ausländischen Diensten muss jedoch ein uneingeschränkter Quellenschutz spielen …« (vgl. BBl 1994 II 1184).

Für eine Harmonisierung spricht, dass sich der im Militärgesetz für den SND verankerte absolute Quellenschutz bewährt hat. Er entspricht sowohl den operativen Bedürfnissen der Sicherheitsorgane, als auch dem bisherigen Verständnis des

Quellenschutzes durch den DAP. Angesichts der mit dem Auslandnachrichtendienst gemachten Erfahrungen hat sich das Argument der operativen Bedürfnisse in diesem doch sehr speziellen Bereich als entscheidend erwiesen. Deshalb ist nicht länger am Konzept des Gesetzes von 1997 festzuhalten. Die Regelung des Quellenschutzes durch das BWIS ist jener der Militärgesetzgebung anzugleichen. Die Formulierung der Gesetzesbestimmung entspricht jener, die in Artikel 99 Absatz 4 des Bundesgesetzes über die Armee und die Militärversicherung (MG; SR 510.19) verwendet wird.

Im Übrigen umfasst Quellenschutz sowohl Geheimhaltung über die Identität der Person, die eine Information mitteilt, als auch über den Inhalt der Information.

2.19 Kapitel 3a Besondere Informationsbeschaffung
Kapitel 3a enthält die entscheidenden Bestimmungen der Revision. Die neuen Bestimmungen ermöglichen es den Sicherheitsorganen, für die präventive Informationsbeschaffung besondere Mittel der Informationsbeschaffung einzusetzen.

Der Titel des Kapitels – Besondere Informationsbeschaffung – entspricht dem Grundgedanken, die dieser Form der Informationsbeschaffung zugrunde liegt. Die Besondere Informationsbeschaffung unterscheidet sich von der in Kapitel 3 geregelten Informationsbeschaffung mit den dort aufgelisteten allgemeinen Mitteln. Die Besondere Informationsbeschaffung erfolgt mit besonderen Mitteln. Der im aktuellen Gesetz enthaltene Ausdruck „Zwangsmassnahmen" schliesst nicht alle im Gesetzesentwurf vorgesehenen besonderen Mittel zusammen. Er wird mit der Aufhebung von Absatz 3 des Artikels 14 aber ohnehin aus dem Gesetz entfernt.

Das Kapitel 3a ist in zwei Abschnitte unterteilt. Der erste Abschnitt ist den allgemeinen Bestimmungen gewidmet, die den Einsatz der Besonderen Informationsbeschaffung regeln; der zweite behandelt die dazu einsetzbaren besonderen Mittel.

2.20 Artikel 18a Grundsatz
In den Bestimmungen dieses Artikels finden sich die Grundlagen der Besonderen Informationsbeschaffung. Die dazu verwendbaren besonderen Mittel werden aufgezählt und es wird bestimmt, in welchen Bereichen sie eingesetzt werden dürfen.

Absatz 1
Die Bestimmungen dieses Artikel bezeichnen den Zweck der Besonderen Informationsbeschaffung: das Erkennen oder Abwehren einer konkreten Gefahr für die innere oder äussere Sicherheit der Schweiz. Diese Bestimmung steht in Beziehung mit dem Buchstaben a von Artikel18b: Schon vor einem Einsatz der besonderen Mittel der Informationsbeschaffung mit dem Ziel, eine Gefahr zu erkennen oder abzuwehren, müssen die Sicherheitsorgane einen Verdacht der Gefährdung der Sicherheit gegen eine bestimmte Person, Organisation oder Gruppierung begründen können (vgl. BGE 109 Ia 273, 288-289: „Die Überwachung darf nicht dazu dienen, einen Verdacht zu begründen").

Die Gefährdungen, zu deren Abwehr die besonderen Mittel der Informationsbeschaffung eingesetzt werden können, sind Terrorismus, verbotener politischer oder militärischer Nachrichtendienst, verbotener Handel mit Waffen, radioaktiven Materialien sowie verbotener Technologietransfer. Weitere

Erläuterungen zu diesen Bereichen finden sich bei Artikel 13a Absatz 1 und insbesondere zum Begriff „Terrorismus“ bei Ziffer 1.2.1.

Absatz 2
Im Absatz 2 werden die Mittel der Besonderen Informationsbeschaffung abschliessend genannt. Weitere Erläuterungen finden sich im Kommentar zu den jeweiligen Mitteln.

2.21 Artikel 18b Voraussetzungen
Für den Einsatz der besonderen Mittel der Informationsbeschaffung müssen fünf Bedingungen kumulativ erfüllt werden.

Absatz 1
Die ersten vier Bedingungen sind materieller Art; sie entsprechen den Anforderungen von Artikel 36 BV. Definiert werden zunächst das öffentliche Interesse und die Umstände, unter denen fallweise eine Einschränkung der Grundrechte gerechtfertigt ist (Buchstabe a). Des Weiteren wird den unterschiedlichen Aspekten des Grundsatzes der Verhältnismässigkeit Rechnung getragen (Buchstaben b – d).

Unter den Begriff des öffentlichen Interesses fallen die Wahrung der inneren und äusseren Sicherheit sowie der Schutz der Mitarbeitenden des Bundesamtes vor Personen, Organisationen und Gruppierungen, von denen angenommen wird, dass sie eine Gefährdung darstellen. Diese Personen, Organisationen und Gruppierungen werden als mutmassliche Gefährder bezeichnet; vgl. Buchstaben a.

Beim Grundsatz der Verhältnismässigkeit gilt es – soweit möglich – zwischen den zugrunde liegenden Komponenten zu unterscheiden: Geeignetheit nach Buchstaben d in initio, wonach das Mittel, das zum Erfüllen des im öffentlichen Interesse verfolgten Zweckes eingesetzt wird, angemessen sein muss; Erforderlichkeit nach Buchstaben c und Buchstaben d in fine, wenn alle herkömmlichen Mittel sich als unwirksam erwiesen haben; Verhältnismässigkeit im engeren Sinne in Buchstabe b, wenn das öffentliche Interesse überwiegt und somit einen Eingriff in die Rechte der betroffenen Person rechtfertigt.

2.22 Artikel 18c Überwachung Dritter und Schutz des Berufsgeheimnisses
Diese Bestimmung regelt zwei besondere Formen der Überwachung: Diejenige von Drittpersonen, die in eine Überwachung involviert sind, ohne dass sie eigentlich Gegenstand der Überwachung sind, und die Überwachung von Personen, die an ein Berufsgeheimnis im Sinne des Artikels 321 des Strafgesetzbuches gebunden sind; ihnen gegenüber müssen bestimmte spezielle Schutzvorkehrungen getroffen werden.

Absatz 1
Die Bestimmung in diesem Absatz regelt den Fall einer indirekten Implikation von Drittpersonen. Es ist denkbar, dass der mutmassliche Gefährder, der Ziel einer Abklärung mit besonderen Mitteln der Informationsbeschaffung ist, Mittel oder Orte benutzt, die nicht ihm gehören, sondern einer Drittperson zur Verfügung stehen; beispielsweise ein Telefon oder ein privates lokales Informationssystem. Dabei ist es durchaus möglich, dass Mittel und Orte ohne Wissen dieser Drittperson benutzt werden. Nichtsdestoweniger müssen diese Kommunikationsmittel und Orte überwacht werden können.

In der Bestimmung kommt klar zum Ausdruck, dass die Drittperson nicht um ihretwillen überwacht wird, solange sie nicht selbst als mutmasslicher Gefährder oder mutmassliche Gefährderin betrachtet wird. Vielmehr ist es ihr Umfeld, das überwacht wird.

Absatz 2
Diese Bestimmung ist nicht auf Drittpersonen beschränkt, sondern regelt jegliche direkte oder indirekte Implikation einer an ein Berufsgeheimnis gebundenen Person, wie etwa ein Anwalt. Diese Bestimmung bezweckt die bestmögliche Wahrung des Berufsgeheimnisses. So gilt die Bestimmung für Dritte, deren Umfeld nach Massgabe des Absatzes 1 überwacht wird, wie auch für die Person, die Ziel einer Aufklärung mit besonderen Mitteln der Informationsbeschaffung ist. Der Text der Bestimmung lehnt sich an den Artikel 4 Absatz 6 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) an. In Übereinstimmung mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (Entscheid Kopp gegen die Schweizerische Eidgenossenschaft, 25 März 1998), muss die Triage von einer Gerichtsbehörde beaufsichtigt werden. Dieser auf ein Strafverfahren gerichtete Entscheid kann analog Verwendung finden. Richtig erscheint deshalb, das Bundesverwaltungsgericht mit dieser Aufgabe zu betrauen (siehe auch die Botschaft zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung vom 1. Juli 1998; BBl 1998 4241, 4323).

2.23 Artikel 18d Bundesverwaltungsgericht
Durch den Einsatz von besonderen Mitteln der Informationsbeschaffung werden Grundrechte eingeschränkt, insbesondere das durch die Artikel 8 EMRK und 13 BV gewährleistete Recht auf Achtung des Privatlebens. Zudem kann sich wegen des Charakters der Besonderen Informationsbeschaffung eine überwachte Person während der Dauer der Massnahme nicht dagegen wehren. Umso wichtiger ist es deshalb, dass die Anwendung der einschlägigen Gesetzesbestimmungen möglichst präzise geregelt und streng kontrolliert wird, ob sie eingehalten werden.

Die Kontrolle erfolgt doppelt und zu unterschiedlichen Zeitpunkten. Personen, gegen die besondere Mittel der Informationsbeschaffung eingesetzt wurden, müssen nach Beendigung des Einsatzes über diese Massnahme unterrichtet werden; sie können dagegen beim Bundesverwaltungsgericht Beschwerde einlegen (nachträgliche Prüfung). Die Pflicht zur nachträglichen Mitteilung von Mitteln der besonderen Informationsbeschaffung an die betroffenen Personen und die Orientierung über die Beschwerdemöglichkeit werden in den Artikeln 18i und 29a geregelt.

Doch damit ist es nicht getan: Zum Zeitpunkt der nachträglichen Mitteilung sind Grundrechte ja bereits eingeschränkt worden. Das Gesetz sieht zudem vor, unter bestimmten Bedingungen vorübergehend oder ganz von der Mitteilung abzusehen (vgl. Artikel 18i Absatz 2). Die nachträgliche Prüfung muss deshalb durch eine vorgängige so ergänzt werden, dass bereits zum Zeitpunkt, in dem der Einsatz von besonderen Mitteln der Informationsbeschaffung beantragt wird, eine strenge Überprüfung stattfindet.

Bei Massnahmen im Rahmen des Strafverfahrens schreibt das Gesetz in der Regel eine doppelte Prüfung vor; durchgeführt wird sie von einer richterlichen Instanz

(Staatsanwalt, Untersuchungsrichter, Tatrichter). Da es sich um gleichartige Eingriffe in Grundrechte handelt, gibt es keinen Grund, für den Einsatz der Besonderen Informationsbeschaffung zu präventiven Zwecken, auf die doppelte Prüfung zu verzichten. Im Grundsatzentscheid aus dem Jahr 1983 (BGE 109 Ia 295) hält das Bundesgericht fest, »dass Missbräuche … im präventiven Bereich noch weit mehr als bei der repressiven Überwachung schädliche Folgen für die freiheitliche, demokratische Ordnung haben können«. Dabei stellt sich die Frage, ob die vorgängige Prüfung einer geplanten Präventivmassnahme einer Gerichtsinstanz vorbehalten bleiben muss, oder ob eine gerichtsinstanzähnliche Stelle damit betraut werden kann, wobei die Mindestanforderung darin besteht, das sie verwaltungsunabhängig ist.

Die Antwort des Europäischen Gerichtshofs für Menschenrechte (EGMR) und jene des Bundesgerichts auf diese Frage sind nicht gänzlich deckungsgleich: Der EGMR hat klar gesagt, dass eine gerichtsinstanzähnliche Stelle ausreicht. Das Bundesgericht scheint daraus eine Prüfung durch eine Gerichtsinstanz abzuleiten.

Im Entscheid Klass gegen die Bundesrepublik Deutschland vom 6. September 1978 befand der EGMR, dass hinsichtlich der präventiven Überwachung das deutsche Gesetz den Anforderungen des Artikels 8 Absatz 2 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) genügt. Darin ist vorgesehen, dass Telefonüberwachungen vorgängig von einem unabhängigen Komitee, bestehend aus drei von einer Bundestagskommission gewählten Mitgliedern, bewilligt werden müssen. Voraussetzung ist indessen, dass das Gesetz dann erlaubt, in die Privatsphäre von Personen einzugreifen, wenn der Eingriff im öffentlichen Interesse gerechtfertigt ist (beispielsweise wegen der nationalen oder öffentlichen Sicherheit), sich in einer demokratischen Gesellschaft als notwendig erweist (vgl. insbesondere den Entscheid Klass, § 21, 53 und 60) und es der Zweck vor dem Hintergrund des Artikel 13 EMRK rechtfertigt (Recht auf wirksame Beschwerde).

Der Gerichtshof bemerkte zwar, dass es an sich wünschenswert wäre, dass in einem Bereich, in dem im Einzelfall zum Nachteil einer demokratischen Gesellschaft grosser Missbrauch betrieben werden könnten, die Prüfung von einem Richter vorgenommen werden würde. Er kam aber zum Schluss, dass mit dem deutschen System eines unabhängigen, wenngleich nicht richterlichen Komitees der Rahmen dessen, was in einer demokratischen Gesellschaft als notwendig gelten kann, nicht gesprengt werde (aaO, § 56).

Die Erwägungen des Bundesgerichts (in BGE 109 Ia 273 ff) legen diejenigen des EGMR etwas anders aus. Es war zu klären, ob ein Gesetz des Kantons Basel-Stadt über die Überwachung zu präventiven und repressiven Zwecken vor Artikel 8 EMRK und Artikel 36 Absatz 4 (Garantie des Briefgeheimnisses) der damals gültigen Bundesverfassung standhielt. »Bei der Beurteilung dieses Verfahrens ist insbesondere in Betracht zu ziehen, dass eine richterliche Behörde die Überwachung genehmigen muss. … Diese weitgehende obligatorische Kontrolle durch eine richterliche Behörde bietet dem Betroffenen … einen hinreichenden Schutz« (BGE 109 Ia 273, 296). Unter Verweis auf diesen Entscheid bekräftigt das Bundesgericht zwölf Jahre später: »die Telephonüberwachung als geheim durchgeführte Massnahme … bedarf einer richterlichen Prüfung« (BGE 122 I 182, 190, T., vom 2. Mai 1996). Im zweiten Fall stand allerdings die Anwendung der Überwachungsmassnahmen in förmlichen Strafverfahren zur Diskussion.

Unklar bleibt indessen, ob sich das Bundesgericht darauf beschränkte, lediglich das Gesetz des Kantons Basel-Stadt zu beschreiben und zum Schluss kam, das Gesetz sei völlig EMRK- und verfassungskonform oder ob das Bundesgericht implizit ausdrücken wollte, dass die Bundesverfassung die Einschaltung eines Richters verlangt, auch wenn die EMRK dies nicht tut (vgl. Entscheid Klass). Anders ausgedrückt, ist aus der Rechtssprechung des Bundesgerichts nicht sicher zu schliessen, ob es mit dem Europäischen Gerichtshof einen Richter als wünschenswert, aber nicht zwingend, oder gestützt auf die Bundesverfassung - strenger als die EMRK - als obligatorisch erachtet.

Angesichts dieser Unklarheit wird im Zuge dieses Gesetzesentwurfs der „Lösung Bundesgericht“ den Vorzug gegeben. Der Entwurf sieht vor, dass das Bundesverwaltungsgericht die Rechtmässigkeit des Einsatzes von besonderen Mitteln der Informationsbeschaffung prüft.

Absatz 1
Absatz 1 legt einerseits den ersten Schritt für den Einsatz von besonderen Mitteln der Informationsbeschaffung fest: Die Antragsstellung erfolgt durch das Bundesamt. Anderseits wird das Bundesverwaltungsgericht für die richterliche Kontrolle dieser und weiterer Anträge für zuständig erklärt und der Prüfauftrag wie folgt umschrieben:

Buchstabe a
Hauptaufgabe des Bundesverwaltungsgerichts ist es, die vom Bundesamt beantragten besonderen Mittel der Informationsbeschaffungen auf ihre Rechtmässigkeit hin zu prüfen. Zu prüfen sind insbesondere das Vorliegen eines öffentlichen Interesses, die Verhältnismässigkeit im Sinne von Artikel 18b und die Beachtung der entsprechenden Gesetzesbestimmungen. Gegenstand der Prüfung sind mithin Gesetzmässigkeit und Verhältnismässigkeit einer geplanten Informationsbeschaffung mit besonderen Mitteln.

Buchstabe b
Eine andere Aufgabe des Bundesverwaltungsgerichts ist die Prüfung, ob die im Gesetz vorgesehenen Bedingungen für eine Mitteilung nach Artikel 18i oder für deren Verzicht erfüllt sind. Auch hier geht es um eine Rechtskontrolle und nicht um die Prüfung der staatspolitischen Opportunität. Letzterer Aspekt liegt in der Zuständigkeit des Departementsvorstehers oder der Departementsvorsteherin EJPD.

Buchstabe c
Eine dritte Aufgabe des Bundesverwaltungsgerichts ist die Prüfung, ob bei der Schaffung von Tarnidentitäten die gesetzlichen Vorgaben eingehalten wurden (vgl. Artikel 14c Absatz 3, 4 und 14d). Dabei geht es um eine Rechtskontrolle, d.h. das Gericht hat sich über das Vorhandensein der in Artikel 14c Absatz 3 und 14d, Absatz 1 und 2 vorgesehenen Bedingungen zu vergewissern. Im Gegenzug spricht es sich nicht über die Opportunität der Schaffung solcher Tarnidentitäten aus; diese Befugnis steht dem Departementsvorsteher oder der Departementsvorsteherin EJPD zu. Auch für die Tarnidentitäten ist die Zustimmung des Bundesverwaltungsgerichts also zwingender Natur. Ihre Schaffung setzt eine positive Stellungnahme des Bundesverwaltungsgerichts voraus (vgl. Artikel 14c Absatz 3 und 14d Absatz 1).

Absatz 2
Absatz 2 stellt klar, dass das Bundesverwaltungsgericht in allen Fällen von Absatz 1 seinen Entscheid nur in Kenntnis aller relevanten Grundlagen fällt. Das heisst, dass das Bundesamt bei Anträgen für den Einsatz von besonderen Mitteln zur Informationsbeschaffung die Zielrichtung nach Artikel 18a, die Voraussetzungen nach Artikel 18b und die Vollzugseinzelheiten nach Artikel 18f Absatz 2 beschreiben muss, bei Anträgen auf Ausnahmen von der Mitteilungspflicht das Vorliegen von Gründen nach Artikel 18i Absatz 2 und bei der Schaffung von Tarnidentitäten die genauen Gründe und Einsatzbereiche nach den Artikeln 14c und d.

Absatz 3
Das Bundesverwaltungsgericht überprüft den vom Bundesamt unterbreiteten Antrag auf dessen Rechtmässigkeit. Es teilt dem Bundesamt seinen schriftlichen und begründeten Entscheid innert 72 Stunden mit; das Bundesamt kann vor einem Entscheid auch um Erläuterungen oder weitere Informationen ersucht werden. Ebenso kann das Bundesverwaltungsgericht einem Antrag bloss teilweise entsprechen oder in seinem Entscheid Auflagen machen.

Eine ganz oder teilweise zustimmende Stellungnahme des Bundesverwaltungsgerichts ist erste, wenngleich auch nicht allein ausreichende Bedingung für den Einsatz von Mitteln der besonderen Informationsbeschaffung. (vgl. Artikel 18e). Damit wird grünes Licht für die Fortsetzung des Genehmigungsverfahrens gegeben; der abschliessende Entscheid, ob einem Antrag stattgeben wird, trifft der Bundesrat.

Der letzte Satz von Absatz 3 legt fest, dass das Bundesverwaltungsgericht das Departement über alle negativen Stellungnahmen unterrichten muss. Mit diesem Vorgehen soll der Departementsleitung eine umfassende Sicht über die vom Bundesamt gestellten Anträge (und nicht nur über die positiven Stellungnahmen) ermöglicht werden.

Absatz 4
Absatz 4 belässt dem Bundesverwaltungsgericht den ihm zukommenden Spielraum bei der internen Organisation und hält lediglich fest, dass die Kontinuität der Rechtsprechung durch die Bezeichnung einer besonders bezeichneten und regelmässig mit Fragen des Staatsschutzes befassten Kammer zu übertragen ist. Ergänzend wird auf die erforderlichen Geheimhaltungserfordernisse hingewiesen, was insbesondere auch ein eigenes Sekretariat rechtfertigt.

Angesichts der auf dem Spiel stehenden Interessen und Rechtsgüter wird sodann auch ohne spezielle gesetzliche Grundlage davon ausgegangen, dass die Behandlung der Fälle einzig durch die zuständigen Richterinnen und Richter erfolgt (Verzicht auf den Einsatz von juristischen Sekretärinnen und Sekretären, Gerichtsschreibern usw.).

2.24 Artikel 18e Entscheid über den Einsatz besonderer Mittel der Informationsbeschaffung

Absatz 1
In diesem Absatz wird verankert, dass das Bundesamt dem Departement bzw. dem Bundesrat nur dann einen Antrag auf Genehmigung des Einsatzes von besonderen

Mitteln der Informationsbeschaffung unterbreiten kann, wenn das Bundesverwaltungsgericht vorher eine positive Stellungnahme abgegeben hat.

Absätze 2 und 3
Liegt eine positive Stellungnahme des Bundesverwaltungsgerichts über die rechtlichen Aspekte des Einsatzes von Mitteln der besonderen Informationsbeschaffung vor, findet anschliessend eine Prüfung nach staatspolitischen Gesichtspunkten statt: Versehen mit der positiven Stellungnahme des Bundesverwaltungsgerichts geht das Dossier an den Departementsvorsteher oder die Departementsvorsteherin des EJPD. Er oder sie konsultiert obligatorisch den Vorsteher oder die Vorsteherin des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) in seiner/ihrer Funktion als Vorsitzende(r) des Sicherheitsausschusses des Bundesrates. Besteht Einigkeit über den Einsatz besonderer Mittel der Informationsbeschaffung, entscheidet der Vorsteher oder die Vorsteherin des EJPD abschliessend. Bei Differenzen entscheidet der Bundesrat über den Antrag. Ungeachtet einer positiven Stellungnahme des Bundesverwaltungsgerichts kann der Departementsvorsteher oder die Departementsvorsteherin des EJPD bzw. der Bundesrat auch ganz oder teilweise auf die beantragte Massnahme verzichten.

Die Auflagen, die das Bundesverwaltungsgericht in einer positiven Stellungnahme vorsehen kann (vgl. Artikel 18d Absatz 3), sind für den Departementsvorsteher oder die Departementsvorsteherin des EJDP bzw. für den Bundesrat verbindlich.

Absatz 4
Erachtet der oder die Departementsvorsteherin des EJPD bzw. der Bundesrat den Einsatz von besonderen Mitteln der Informationsbeschaffung für angezeigt, präzisieren sie die Modalitäten (Buchstaben a bis e). Zu konkretisieren sind insbesondere

- das angestrebte Ziel,
- das Zielobjekt (d.h. der mutmassliche Gefährder),
- die nach Artikel 18a Absatz 2 einsetzbaren Mittel,
- die Dauer des Einsatzes: Das Gesetz sieht eine erste Frist von höchstens sechs Monaten vor (vgl. Absatz 4). Bestimmte Operationen – beispielsweise das Durchsuchen eines Informationssystems – erstrecken sich nicht über eine längere Zeit, sondern lassen sich möglicherweise in einem Mal erledigen. Für diesen Fall sieht der Gesetzesentwurf die Festlegung einer Frist vor. Es gilt dann, einen Zeitpunkt zu bestimmen, bis zu dem die Operation abgeschlossen sein sollte. Begrenzt ist damit nicht die Zeit, während der die Besondere Informationsbeschaffung stattfindet, sondern die Dauer, während der die Genehmigung gültig ist.
- und die mit der Durchführung verbundenen Auflagen (regelmässige Berichterstattung).

Absatz 5
Die vom Departementsvorsteher oder der Departementsvorsteherin des EJPD bzw. vom Bundesrat bewilligte Frist kann beim Vorliegen einer positiven Stellungnahme des Bundesverwaltungsgerichts zwei Mal und um jeweils drei Monate verlängert werden. Das bedeutet, dass ein besonderes Mittel während höchstens zwölf Monaten (6 + 3 + 3) eingesetzt werden kann. Sollte es länger benötigt werden, hat das Bundesamt bzw. das Departement neu Antrag zu stellen.

Absatz 6
Absatz 6 beschreibt das Verhältnis zu den Verfassungskompetenzen des Bundesrates und ist deklaratorischer Natur. Das im BWIS vorgesehene Verfahren ersetzt die in der Schweizerischen Bundesverfassung (BV) vorgesehenen verfassungsunmittelbaren Kompetenzen des Bundesrates nicht. Vielmehr tritt das Verfahren nach BWIS ergänzend hinzu, indem es gesetzliche Grundlagen für den Normalfall schafft. In aussergewöhnlichen Lagen kann der Bundesrat deshalb auch inskünftig namentlich nach Artikel 185 Absatz 3 BV vorgehen, soweit die dort verankerten Voraussetzungen zur Abwehr einer unmittelbar drohenden Gefahr der inneren oder äusseren Sicherheit gegeben sind. Rein theoretisch ist es also möglich, dass es für die Anordnung von Mitteln der besonderen Informationsbeschaffung an den gesetzlichen Anordnungsvoraussetzungen mangelt und deshalb das Bundesamt keinen Antrag stellt oder das Bundesverwaltungsgericht eine negative Stellungnahme erlässt, es hingegen zulässig und geboten ist, dass der Bundesrat wegen dem Vorliegen einer andersartigen, vom BWIS nicht erfassten Bedrohung bzw. der Schwere des Falles verfassungsunmittelbare Massnahmen anordnet. Erweist sich also angesichts besonderer Umstände ein Regierungsakt als notwendig, obliegt es dem Bundesrat, insbesondere nach Massgabe von Artikel 185 Absatz 3, BV, die politische Verantwortung zu übernehmen, und den Einsatz eines besonderen Mittels anzuordnen.

2.25 Artikel 18f Dringlichkeitsverfahren
Als Ausnahme ist in Artikel 18f der Fall definiert, in dem Gefahr im Verzug ist. Wenn der Erfolg von Mitteln der besonderen Informationsbeschaffung durch ein Abwarten des Entscheids des Bundesverwaltungsgerichts, des Departementsvorstehers oder der Departementsvorsteherin EJPD oder des Bundesrates gefährdet oder verunmöglicht würde, soll rasch gehandelt werden können. Dies ist etwa dann der Fall, wenn eine wichtige Zielperson überraschend in die Schweiz einreist und ab der Einreise intensiv – beispielsweise auch durch Kontrolle des Fernmeldeverkehrs – überwacht werden muss.

Absatz 1
Die besonderen Mittel der Informationsbeschaffung werden in Dringlichkeitsfällen vom Direktor oder der Direktorin des Bundesamtes unmittelbar angeordnet; sie können sofort vollzogen werden. Auch in dringlichen Fällen müssen die materiellen Voraussetzungen (Artikel18b Absatz 1 Buchstaben a bis d) für den Einsatz eines besonderen Mittels erfüllt sein. Es obliegt dem Direktor oder der Direktorin des Bundesamtes sicherzustellen, dass die Voraussetzungen auch tatsächlich gegeben sind. Gleichzeitig erfolgt eine Orientierung des Departements.

Absatz 2
Der Direktor des Bundesamtes ist verpflichtet, dem Bundesverwaltungsgericht den üblichen Antrag innert 24 Stunden nachzureichen, wobei die Dringlichkeit gesondert zu begründen ist. Alsdann nimmt das Verfahren seinen normalen Lauf. Der Entscheid des Bundesverwaltungsgerichts hat wie beim „normalen“ Verfahren innert 72 Stunden zu erfolgen.

Absatz 3
Der Antrag des Bundesamtes für eine nachträgliche Genehmigung des Einsatzes von besonderen Mitteln der Informationsbeschaffung setzt eine positive

Stellungnahme des Bundesverwaltungsgerichts voraus. Die Antragsstellung hat umgehend – also rasch - zu erfolgen.

Absatz 4
Verweigert das Bundesverwaltungsgericht eine positive Stellungnahme oder lehnt der Departementsvorsteher oder die Departementsvorsteherin des EJPD bzw. der Bundesrat die nachträgliche Genehmigung der dringlich angeordneten besonderen Mitteln der Informationsbeschaffung ab, muss das Bundesamt sämtliche aus dieser Informationsbeschaffung stammenden und bis dahin erhobenen Daten unverzüglich vernichten (vgl. die analoge Bestimmung von Artikel 7 Abs. 4 BÜPF).

2.26 Artikel 18g Einstellung des Einsatzes
Wird die Informationsbeschaffung nicht mehr benötigt (Buchstabe a), ist sie aussichtslos (Buchstabe b), wird sie nicht verlängert (Buchstabe c) oder wird sie, im Falle eines dringlichen Verfahrens, vom Bundesverwaltungsgericht als nicht rechtmässig beurteilt oder vom Departementsvorsteher oder der Departementsvorsteherin des EJPD bzw. vom Bundesrat nicht genehmigt (Buchstaben d und e), so stellt sie das Bundesamt umgehend ein. Wird die Genehmigung für eine bereits in Vollzug stehende Massnahme verweigert, dürfen die Erkenntnisse aus dieser Massnahme nicht verwendet werden. Hat das Bundesamt aufgrund dieser Massnahme gewonnene Erkenntnisse bereits an andere Organe oder Behörden weitergegeben, muss es sie auffordern, Aufzeichnungen über diese Erkenntnisse zu vernichten. Diese Bestimmungen entsprechen den allgemein geltenden datenschutzrechtlichen Grundsätzen bei der Bearbeitung von Personendaten.

2.27 Artikel 18h Bearbeiten der mit besonderen Mitteln beschafften Personendaten
Diese Bestimmung regelt die Bearbeitung von Personendaten, die mit besonderen Mitteln der Informationsbeschaffung gewonnen wurden.

Absatz 1
Diese Bestimmung regelt die Rahmenbedingungen für die Aufbewahrung der in Artikel 15 BWIS aufgelisteten Daten. Die gesammelten Daten müssen innerhalb von dreissig Tagen, nachdem ein Einsatz endet, vernichtet werden, wenn sie keinen Bezug zur Gefährdung aufweisen, wegen der die besonderen Mittel der Informationsbeschaffung zum Einsatz angeordnet wurden.

Absatz 2
In diesem Absatz wird festgelegt, dass sich die Bearbeitung der mit besonderen Mitteln der Informationsbeschaffung erhobenen Personendaten nach Artikel 3 Absätze 1-3 und den Artikeln 15, 16 und 17 BWIS richtet.

2.28 Artikel 18i Mitteilungspflicht
Diese Bestimmung ist ein zentrales Element des Gesetzesentwurfs und massgeblich für die Ausgestaltung der nachträglichen Prüfung (siehe Kommentar zum Artikel 18d in initio). Unterrichtet das Bundesamt nach Abschluss eines Einsatzes die betroffene Person nicht darüber, dass über sie mit besonderen Mitteln Informationen gesammelt wurde, hat sie in der Regel keine Möglichkeit, sich nachträglich dagegen zu wehren, es sei denn, sie habe auf anderem Weg davon erfahren. Mit der Information der

Betroffenen wird diesen ermöglicht, ihr Beschwerderecht vor Gericht wahrzunehmen (vgl. Artikel 29a).

Die Pflicht, Betroffene zu informieren, ist verfassungsrechtlicher Natur, und ergibt sich implizit aus der Garantie der Achtung des Privatlebens einer Person und ihres Briefverkehrs. Diese Garantie gründet in den Artikeln 8 EMRK und 13 BV. In einem Strafverfahren überlagern sich das Recht auf Auskunft und der Anspruch auf rechtliches Gehör (Art. 29 BV). Im Zusammenhang mit einer präventiven Operation, aus der keine Strafverfolgung resultiert, kann es aber vorkommen, dass das als Grundlage für die Operation dienende Gesetz keine Pflicht zur Information der Betroffenen enthält. Dies war der Fall beim Gesetz des Kantons Basel-Stadt, um das es im erwähnten Entscheid vom November 1983 ging. Das Gesetz besagte lakonisch: »Das Verfahren ist … gegenüber dem Betroffenen geheim« (BGE 109 Ia 273, 276). Demgegenüber hielt das Bundesgericht fest, die Bundesverfassung verbiete es, »dass von einer nachträglichen Bekanntgabe generell in jedem Fall abgesehen wird. … Demnach ist vielmehr zu fordern, dass den Betroffenen grundsätzlich von den durchgeführten Überwachungsmassnahmen nachträglich Kenntnis gegeben wird. Dies hat für die präventive und die repressive Überwachung sowie gegenüber den Angeschuldigten und Verdächtigten und Drittpersonen zu gelten. … „. Demnach ist grundsätzlich von der Pflicht auszugehen, Überwachungsmassnahmen den Betroffenen bekannt zu geben (BGE 109 Ia 273, 298-299).

Absatz 1
In Befolgung dieser Rechtsprechung wird im vorliegenden Gesetzesentwurf der Grundsatz der nachträglichen Mitteilungspflicht verankert. Ist eine Operation beendet, muss das Bundesamt grundsätzlich Betroffene über die Informationsbeschaffung unterrichten (zum Begriff der Operation siehe Artikel 14 der Verordnung über Massnahmen zur Wahrung der inneren Sicherheit vom 27. Juni 2001, SR 120.2).

Absatz 2
Im erwähnten Entscheid Klass (§§ 57 bis 59, siehe Kommentar zu Artikel 18d) stellte der Europäische Gerichtshof für Menschenrecht (EGMR) fest, dass eine nachträgliche Mitteilung sehr wohl den langfristigen Zweck einer Überwachung in Frage stellen könne. Ausserdem bestehe die Gefahr, dass die Arbeitsmethoden von Nachrichtendiensten, die überwachten Bereiche und gegebenenfalls sogar die Identität von Ermittelnden preisgegeben werden. So wurden die Ausnahmen, die das deutsche Gesetz für die Mitteilungspflicht vorsah, für rechtmässig befunden.

In seinem Entscheid aus dem Jahr 1983 folgte das Bundesgericht diesen Erwägungen (BGE 109 Ia 273, 300-301) und anerkannte nahezu die gleiche Art von Ausnahmen. Es hielt dafür, dass »diese Ausnahmen … allerdings streng anzuwenden« seien. In der Praxis wird – ungeachtet dieses mahnenden Vorbehaltes – die Mitteilungspflicht durch die Erfordernisse der polizeilichen Fahndung relativiert. Die im Absatz 2 unter den Buchstaben a bis d aufgeführten Ausnahmen sind weitgehend dem Artikel 10 Absatz 3 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1) und dem Artikel 22 Absatz 2 des Bundesgesetzes vom 20. Juni 2003 über die verdeckte Ermittlung nachgebildet (SR 312.8).

Die Gründe, welche den Verzicht oder den Aufschub der Mitteilungspflicht rechtfertigen, werden in Buchstaben a – d abschliessend aufgezählt.

Im Übrigen liegt es nicht in der Kompetenz des Bundesamtes, die Mitteilung aufzuschieben oder ganz davon abzusehen. Da ein verfassungsmässiges Recht eingeschränkt wird, muss verfahrensmässig sichergestellt werden, dass das Individualinteresse des Einzelnen, sich gegen Eingriffe in seine Privatsphäre wehren zu können, nur dann beschränkt werden kann, wenn ein vorrangiges öffentliches Interesse einen Aufschub oder Verzicht der Mitteilung klar notwendig macht. Dieses Abwägen der gegenseitigen Interessen ist umso heikler, als das Mitteilungsverfahren auch die Möglichkeit vorsieht, bei einer richterlichen Behörde die Rechtmässigkeit des Einsatzes von Mitteln der besonderen Informationsbeschaffung überprüfen zu lassen. Es rechtfertigt sich deshalb, für das Verweigern oder Aufschieben der Mitteilungspflicht strenge Regeln vorzusehen: Gegebenenfalls stellt das Bundesamt begründeten Antrag, warum von einer Mitteilung abgesehen werden soll. Anschliessend findet eine Rechtskontrolle durch das Bundesverwaltungsgericht statt. Gibt dieses eine positive Stellungnahme ab, entscheidet der Departementsvorsteher oder die Departementsvorsteherin EJPD abschliessend über die Zulässigkeit, von einer Mitteilung abzusehen.

Mit der Konsultation des Vorstehers oder der Vorsteherin des VBS nach Artikel 18e Absatz 2 des vorliegenden Entwurfs ist auch sichergestellt, dass allfällige Geheimhaltungsbedürfnisse des Auslandnachrichtendienstes (SND) frühzeitig Eingang in die Akten finden können und beim Entscheid des Bundesverwaltungsgerichts bzw. des Departementsvorstehers oder der Departementsvorsteherin EJPD mitberücksichtigt werden können.

Das Recht auf Auskunft im Sinne des Artikels 8 und folgende des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (SR 235.1) richtet sich nach Artikel 18 BWIS.

2.29 Artikel 18j Vollzug durch die Kantone
Dieser Artikel besagt, dass die im Auftrag des Bundes und von den Sicherheitsorganen der Kantone mit besonderen Mitteln durchgeführte Informationsbeschaffung sich nach den Bestimmungen des BWIS richtet. Das heisst, wenn Sicherheitsorgane der Kantone im Auftrag des Bundes nicht allgemein zugängliche Orte überwachen oder dort Überwachungsgeräte installieren, sind die Bestimmungen der Artikel 18a ff dieses Gesetzesentwurfes und nicht Bestimmungen des kantonalen Rechts massgebend.

2.30 2. Abschnitt Besondere Mittel der Informationsbeschaffung
Gemäss den Artikeln 36 Absatz 1 und 164 Absatz 1 Buchstaben a BV müssen schwerwiegende Einschränkungen der Grundrechte im Gesetz vorgesehen sein. Es genügt indessen nicht, die verschiedenen, die Grundrechte möglicherweise einschränkenden Mittel lediglich aufzulisten. Vielmehr gilt es, im Einzelnen das Ausmass der Einschränkungen darzulegen, in diesem Zusammenhang darauf hinzuweisen, worauf sie sich erstrecken, und wichtige Einzelheiten der zulässigen Handlungen zu regeln. Diese Regelungen sind umso grundlegender, als dass ihre Anwendung variiert, je nachdem, ob die Mittel in einem Strafverfahren oder zur nachrichtendienstlichen Informationsbeschaffung eingesetzt werden. So wird beispielsweise – sofern keine detaillierten, gesetzlich definierten Umstände vorliegen

– im Zuge eines strafrechtlichen Ermittlungsverfahrens ein Informationssystem im Beisein der verdächtigen Person oder einer sie vertretenden Person durchsucht. Im Bereich der nachrichtendienstlichen Beschaffung müsste dasselbe Informationssystem indessen ohne das Wissen der betroffenen Person durchsucht werden können.

2.31 Artikel 18k Überwachen des Post- und Fernmeldeverkehrs

Die Überwachung des Post- und Fernmeldeverkehrs zu Zwecken der Strafverfolgung wird im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1) geregelt. Das hier zu regelnde präventive Überwachen wird jedoch nicht zum Zweck der Strafverfolgung durchgeführt, sondern zur Erkennung von konkreten Gefährdungen durch Terrorismus, verbotenen politischen und militärischen Nachrichtendienst und verbotenen Handel mit Waffen und radioaktiven Materialien sowie durch verbotenen Technologietransfer. Deshalb muss sie im BWIS besonders geregelt werden.

Das BWIS soll aber nur besondere Regeln aufstellen, wo Abweichungen oder Präzisierungen zum BÜPF notwendig sind. Für technische und organisatorische Fragen verweist es auf das BÜPF, weil nicht beabsichtigt ist, für die präventiven Überwachungen grundsätzlich andere Verfahren und technische Anforderungen zu definieren. Vielmehr sollen die bewährten Strukturen benutzt werden.

Absatz 1

In diesem Absatz wird der Zweck der Post- und Fernmeldeüberwachung beschrieben: Genannt werden Kommunikationsmittel im Allgemeinen. Wie im Fernmeldegesetz und im BÜPF werden bewusst keine technischen Mittel im Einzelnen genannt, um in diesem Gebiet, in dem die technische Entwicklung besonders rasant voranschreitet, die nötige Handlungsfreiheit nicht zu verlieren. Der Artikel hält des Weiteren fest, dass es konkreter Hinweise bedarf, die vermuten lassen, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin diese Mittel dazu benützen, um mit Personen Informationen auszutauschen oder Handlungen zu vollziehen, die einen ebenfalls direkten Bezug zu der konkreten Gefährdung der inneren oder äusseren Sicherheit aufweisen. Damit zu einem gegebenen Zeitpunkt eine Überwachung gerechtfertigt ist, müssen diese Hinweise hinreichend konkret und aktuell sein.

Absatz 2

Die Bestimmung betreffend die Überwachung einer öffentlichen Fernmeldestelle entspricht der Sonderregelung von Artikel 4 Absatz 2 BÜPF. In der Praxis handelt es sich um Fälle, in denen beispielsweise aus der Observation einer Zielperson oder aus anderen Fernmeldeüberwachungen bekannt ist, dass eine Zielperson regelmässig oder mit Blick auf eine ganz bestimmte Gelegenheit eine bestimmte öffentliche Telefonzelle benutzt.

Absatz 3

Wenn eine Zielperson den Fernmeldeanschlusses in rascher Folge wechselt, zum Beispiel durch den Einsatz von Prepaid-Karten in der Mobiltelefonie, käme eine Anordnung im Einzelfall fast immer zu spät. In diesen Fällen kann eine Anordnung getroffen werden, dass alle identifizierten Anschlüsse, welche die Person oder Organisation benutzt, überwacht werden können. Auch diese Bestimmung hat ihr Vorbild im BÜPF (Artikel 4 Absatz 4).

Absatz 4

Für die Durchführung der präventiven Post- und Fernmeldeüberwachungen sollen keine Parallelstrukturen zum BÜPF geschaffen werden. Deshalb gilt für die Formen der Überwachung, ihre technische Umsetzung und die Entschädigungen das Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs und dessen Ausführungserlasse sinngemäss.

Öffentliches Interesse und Verhältnismässigkeit

Die Überwachung des Post- und Fernmeldeverkehrs stellt eine schwerwiegende Einschränkung in die Privatsphäre dar. Nach Artikel 36 BV müssen Einschränkungen von Grundrechten durch ein öffentliches Interesse gerechtfertigt sein und im Vergleich zum angestrebten Zweck verhältnismässig sein. Hinsichtlich der Rechtfertigung durch ein öffentliches Interesse darf das Mittel der Überwachung des Post- und Fernmeldeverkehr wie auch alle anderen besonderen Mittel nur in den drei Bereichen eingesetzt werden, aus denen eine Gefährdung entstehen kann, die an die Grundstrukturen unserer Gesellschaft rührt (vgl. Kommentar zu Artikel 13a Absatz 1). Es lässt sich somit nicht in Abrede stellen, dass das öffentliche Interesse diese Massnahme rechtfertigt. Um die Verhältnismässigkeit der Massnahme beurteilen zu können, gilt es zu prüfen, ob sie angemessen und notwendig ist und ob sie im engeren Sinn des Wortes in einem vernünftigen Verhältnis zum angestrebten Zweck steht. Liegen hinreichende Anhaltspunkte vor, dass der mutmassliche Gefährder für seine Umtriebe Fernmeldemittel benutzt, stellt diese Form der Überwachung das angemessene Mittel dar, um Informationen zu gewinnen, anhand derer die Gefährdung besser beurteilt und ihr vorgebeugt werden kann.

Die Sicherheitsorgane sind indessen nicht berechtigt, Überwachungen im Sinne einer reinen Sondierung, das heisst gewissermassen auf gut Glück, durchzuführen, nur weil Grund zur Annahme besteht, dass eine Person eine Gefahr für die innere Sicherheit darstellen könnte. Es bedarf in jedem Fall konkreter Anhaltspunkte, die darauf schliessen lassen, dass die jeweilige Person für ihre Umtriebe sich bestimmter Fernmeldemittel bedient. Ist glaubhaft dargelegt, dass für die gefährdenden Umtriebe Fernmeldemittel verwendet werden, gilt die Überwachungsmassnahme als angemessen.

Was die Notwendigkeit der Massnahme angeht, so ist es offensichtlich, dass die Kontakte einer Person, von der eine Gefahr auszugehen scheint, oder der Inhalt der über Fernmeldemittel ausgetauschten Mitteilungen sich einzig mittels der Fernmeldeüberwachung in Erfahrung bringen lassen. Mit der allgemeinen Informationsbeschaffung gemäss Artikel 14 Absatz 2 lassen sich solche erforderlichen Informationen kaum beschaffen.

Ob die Massnahme im engen Sinn des Wortes verhältnismässig ist, dass heisst, ob das öffentliche Interesse in dem Masse überwiegt, das der Eingriff in die Grundrechte der Person gerechtfertigt ist, lässt sich nicht allgemein-abstrakt festlegen. Nur in Kenntnis der fallspezifischen Umstände können die verantwortlichen Organe zwischen öffentlichem Interesse und der Wahrung der Grundrechte des Einzelnen abwägen und einen fundierten Entscheid zu fällen. Wichtig ist, dass nicht allein die Sicherheitsorgane, sondern eine unabhängige richterliche Instanz die rechtlichen Aspekte beurteilt. Eine solche ist am besten in der Lage, die Bedürfnisse der Sicherheitsorgane und den legitimen Anspruch Aller, sich ohne staatliche

Einmischung mit anderen zu kommunizieren und Kontakte zu pflegen, gegeneinander abzuwägen. Im Rahmen dieser Erwägungen und in Berücksichtigung der Einschränkungen und Vorkehrungen, die der Gesetzesentwurf vorsieht, ist die präventive Überwachung des Post- und Fernmeldeverkehrs eine zur Wahrung des öffentlichen Interesses verhältnismässiges Mittel, das in Übereinstimmung mit den Anforderungen der Verfassung und der Menschenrechtskonventionen eingesetzt werden kann.

2.32 Artikel 18l Beobachten an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät

Nach den geltenden Bestimmungen des BWIS dürfen die Sicherheitsorgane an öffentlichen und allgemein zugänglichen Orten Vorgänge beobachten und diese auch mit Bild- und Tonaufzeichnungen festhalten (Artikel 14 Absatz 2 Buchstaben f BWIS). Mit der neuen Bestimmung soll es nun möglich werden, auch an nicht allgemein zugänglichen Orte zu beobachten und aufzuzeichnen (beispielsweise in gewerbsmässig genutzten Räumen, Versammlungslokalen, Wohnungen, Hotelzimmern; vgl. Absatz 1). Dazu ist neu auch der Einsatz technischer Überwachungsgeräte vorgesehen (vgl. Absatz 2). Nach geltendem Recht ist es verboten, solche Mittel einzusetzen, um nicht öffentliche Gespräche abzuhören oder aufzuzeichnen (vgl. Artikel 179bis und 179ter StGB). Verboten ist auch, einen Vorgang aus dem Geheim- oder Privatbereich einer Person mit einem Aufnahmegerät zu beobachten oder aufzuzeichnen (Artikel 179^{quater} StGB), wenn sich zwar ein solcher Vorgang in einem allgemein zugänglichen Ort abspielt, aber von den Beteiligten willentlich der Öffentlichkeit entzogen wird. Nicht geschützt dagegen ist allgemeines privates Verhalten in der Öffentlichkeit.

Absatz 1

Diese Bestimmung legt die Einzelheiten der Beobachtung fest und umschreibt die Bedingungen, unter denen sie durchgeführt werden darf. Es müssen konkrete und aktuelle Tatsachen vorliegen, die vermuten lassen, dass die betreffende Person einen bestimmten Ort nutzt, um mit anderen zu kommunizieren oder um Handlungen zu vollziehen, die einen direkten Bezug zu der konkreten Gefährdung der inneren oder äusseren Sicherheit aufweist.

Absatz 2

Der Einsatz technischer Überwachungsgeräte entspricht in Regelung und Umfang der Bestimmung von Artikel 66 Absatz 2 der Bundesstrafprozessordnung (SR 312.0). Es handelt sich um akustische und optische Beobachtungs- und Aufzeichnungsgeräte. Diese Geräte können bei Vorliegen der entsprechenden Voraussetzungen auch in einem privaten Umfeld eingesetzt werden. Ebenfalls unter diese Bestimmung fällt das technische Beobachten und Aufzeichnen von Vorgängen, die privater Natur sind, obwohl sie sich an einem allgemein zugänglichen Ort abspielen, wie etwa ein privates Gespräch in einem Restaurant.

Öffentliches Interesse und Verhältnismässigkeit

Das Beobachten an einem nicht allgemein zugänglichen Ort oder mithilfe technischer Überwachungsgeräte stellt eine schwerwiegende Einschränkung der Privatsphäre dar. Wie bereits erwähnt, muss nach Artikel 36 BV ein solcher Eingriff durch ein öffentliches Interesse gerechtfertigt sein und im Verhältnis zum angestrebten Zweck stehen. Hinsichtlich der Rechtfertigung dieses besonderen Mittels durch ein öffentliches Interesse sei auf die Erwägungen zu den Artikeln 13a und 18k

verwiesen. Zur Frage der Verhältnismässigkeit lassen sich die folgenden Überlegungen anstellen: Lässt sich aufgrund hinreichender Tatsachen feststellen, dass der mutmassliche Gefährder oder die mutmassliche Gefährderin für seine oder ihre Umtriebe einen bestimmten Ort nutzt, stellt die Beobachtung das angemessene Mittel dar, um nützliche Informationen zu gewinnen, anhand derer die Gefährdung beurteilt und ihr vorgebeugt werden kann. Die Sicherheitsorgane sind indessen nicht berechtigt, das gesamte private Umfeld einer Person zu beobachten, nur weil Grund zur Annahme besteht, dass sie eine Gefahr für die innere Sicherheit darstellen könnte. Die Beobachtung muss auf ein bestimmtes, konkretes Ziel ausgerichtet sein, das zentraler strategischer Bestandteil der Handlungen des mutmasslichen Gefährders ist. Lässt sich zwischen den als Gefahr erachteten Handlungen und der Nutzung eines Ortes ein Bezug hinreichend glaubhaft belegen, kann die Massnahme als angemessen bezeichnet werden. Bezüglich der Notwendigkeit ist offensichtlich, dass sich abgesehen vom allfälligen Einsatz eines Informanten oder einer Informantin mit der allgemeinen Informationsbeschaffung nach Artikel 14 Absatz 2 BWIS keine Informationen über Vorgänge beschaffen lassen, die sich in Privaträumen abspielen. Nur ist es nicht immer möglich, in solchen Situationen Informanten zu gewinnen oder einzusetzen. Die Verhältnismässigkeit im engeren Sinn des Wortes, das heisst, das Abwägen, ob das öffentliche Interesse dasjenige der betroffenen Person überwiegt, lässt sich wie bereits gesagt, nur im konkreten Fall von den verantwortlichen Organen beurteilen. Die Entscheidung, ob in einem Fall ein rechtmässiges überwiegendes öffentliches Interesse besteht, ist dem Bundesverwaltungsgericht vorbehalten.

Der Einsatz technischer Überwachungsgeräte ist weniger ein eigenständiges Überwachungsmittel als vielmehr ein Hilfsmittel zur Beobachtung von Vorgängen, die sich in der Privatsphäre abspielen. Bei der mithilfe technischer Mittel durchgeführten Beobachtung treten diese Mittel lediglich an die Stelle einer beobachtenden Person, die in einem privaten Raum physisch gegenwärtig ist. Daraus folgt, dass aus denselben Gründen, aus denen das Beobachten von Vorgängen in einem privaten Raum als verhältnismässig bezeichnet werden kann, die mithilfe technischer Geräte durchgeführte Beobachtung a priori als Mittel erachtet werden kann, das demselben Grundsatz der Verhältnismässigkeit entspricht. Ob ein überwiegendes öffentliches Interesse vorliegt, wird je nach Sachlage zu entscheiden sein.

2.33 Artikel 18m Geheimes Durchsuchen eines Datenverarbeitungssystems

Die Nutzung von moderner EDV-Infrastruktur nimmt im täglichen Leben eine immer wichtigere Rolle ein. Gerade das Internet ist zu einem wichtigen Ort des Austauschs von Informationen geworden. Weil das öffentliche Internet von Sicherheitsbehörden heute bereits intensiv zur Informationsbeschaffung konsultiert wird, verlagern relevante Gruppen (etwa Terrororganisationen) die Verbreitung von heiklen Inhalten zunehmend in geschützte Bereiche, zu denen der Zugang beispielsweise mit Passwörtern geschützt ist. Ein Eindringen ist hier mit entsprechendem Fachwissen zwar möglich, jedoch strafrechtlich verboten (Artikel 143bis StGB, unbefugtes Eindringen in ein Datenverarbeitungssystem).

Die Bestimmung beschreibt, worum es sich bei diesem Mittel der besonderen Informationsbeschaffung handelt und wie es eingesetzt werden kann. Der Geltungsbereich erstreckt sich in Anlehnung an die entsprechenden Bestimmungen des Strafgesetzbuches (vgl. Artikel 143 und 143bis StGB) auf elektronisch oder in vergleichbarer Weise gespeicherte Daten, die besonders gegen Zugriff Fremder

gesichert sind. Im Gegensatz der im Rahmen einer Strafuntersuchung durchgeführten Durchsuchung, wird hier die Durchsuchung ohne das Wissen des mutmasslichen Gefährders durchgeführt. Es müssen wiederum hinreichend klare und aktuelle Tatsachen vorliegen, die vermuten lassen, dass die betreffende Person ein bestimmtes Datenverarbeitungssystem für ihre Umtriebe nutzt. Die Durchsuchung hat aber passiven Charakter. Das heisst, sie erlaubt nicht, so in das System einzugreifen, dass es funktionsuntüchtig wird oder seine Funktionen gestört oder Daten vernichtet werden. Zu denken ist etwa an die Suche nach Kontaktadressen im Laptop eines mutmasslichen Gefährders oder den Klartext einer chiffriert übermittelten E-Mail.

Öffentliches Interesse und Verhältnismässigkeit
Das Durchsuchen eines Datenverarbeitungssystems stellt eine schwerwiegende Einschränkung der Privatsphäre dar. Wie erwähnt muss gemäss Artikel 36 BV eine solche Einschränkung durch ein öffentliches Interesse gerechtfertigt sein und im Verhältnis zum angestrebten Zweck stehen. Hinsichtlich der Rechtfertigung dieses Mittels der Besonderen Informationsbeschaffung durch ein öffentliches Interesse sei auf die Erläuterungen zu den Artikeln 13a und 18l verwiesen. Bezüglich der Verhältnismässigkeit gilt Folgendes: Lässt sich mit einiger Wahrscheinlichkeit erkennen, dass der mutmassliche Gefährder ein System und Datennetze nutzt, um für sich oder Dritte Daten zu speichern, die die innere oder äussere Sicherheit konkret gefährden, ist die Durchsuchung eines solchen Systems ein angemessenes und notwendiges Mittel, um die zur Beurteilung der Gefährdung notwendigen Informationen zu beschaffen. Es gibt kein anderes Mittel als in das Datenverarbeitungssystem einzudringen, um auf diese Daten zuzugreifen. Nur Datenverarbeitungssysteme sollen durchsucht werden, nicht aber Räume oder Fahrzeuge. Für diese sollen zum Zweck der Informationsbeschaffung lediglich andere Mittel zur Verfügung stehen, wie die physische Beobachtung oder technische Überwachungsgeräte. Die Revision schränkt hier die Auswahl an vorgesehenen Mitteln ein, um schon auf dieser Ebene die Verhältnismässigkeit zu wahren. Die Verhältnismässigkeit im engeren Sinn des Wortes, das heisst, das Abwägen, ob das öffentliche Interesse über dasjenige der betroffenen Person überwiegt, lässt sich wie bereits gesagt, nur im konkreten Fall von den verantwortlichen Organen beurteilen. Die Entscheidung, ob im konkreten Fall ein rechtmässiges überwiegendes öffentliches Interesse besteht, ist dem Bundesverwaltungsgericht vorbehalten.

2.34 Kapitel 3b Verbot von Tätigkeiten
An dieser Stelle wird das Verbot als neue Massnahme eingeführt. Das heutige Gesetz beschränkt sich auf die Regelung der Bearbeitung von Personendaten durch die Sicherheitsorgane und den Erlass von Bestimmungen, die auf der Amtshilfe gründen. Bestimmungen, die das Verhalten von Personen lenken, enthält es keine. Die vom Parlament am 24. März 2006 verabschiedete Revision des BWIS (Gewaltpropaganda, Gewalt bei Sportveranstaltungen) ist ein erster Schritt in diese Richtung. Sie sieht Massnahmen gegen Gewalttätigkeiten an Sportveranstaltungen vor, so insbesondere Vorschriften, die das Verhalten von Privatpersonen lenken sollen: Rayonverbot, Ausreisebeschränkung, Meldeauflage und Polizeigewahrsam. Die vorliegende Revision geht auch in diese Richtung. Die präventive Gefahrenabwehr soll gestärkt werden, indem die Möglichkeit geschaffen wird, unmittelbar auf das Verhalten von Privatpersonen zu reagieren.

2.35 Artikel 18n
Mit dieser Bestimmung erhält der Departementsvorsteher oder die Departementsvorsteherin die Kompetenz, gegen bestimmte Tätigkeiten gerichtete verwaltungsrechtliche Verbote zu verhängen, soweit die fragliche Tätigkeit mit einer konkreten Gefährdung der inneren oder äusseren Sicherheit der Schweiz verbunden ist. Nach heutigem Recht können solche Verbote nur gestützt auf die Bundesverfassung verhängt werden. Sie ermächtigt den Bundesrat, Verordnungen und Verfügungen zur Wahrung der Landesinteressen zu erlassen (Artikel 184 Absatz 3 BV) und Massnahmen gegen unmittelbar drohende schwere Störungen der öffentlichen Ordnung oder der inneren oder äusseren Sicherheit der Schweiz zu treffen (Artikel 185 Absatz 3 BV). Alle auf diesen beiden verfassungsrechtlichen Bestimmungen gestützten Verordnungen müssen indessen befristet werden und können nicht auf unbegrenzte Zeit immer wieder verlängert werden. Andernfalls würde die Verfassung ausgehöhlt. Deshalb soll auf Gesetzesebene eine Möglichkeit geschaffen werden, bei gegebener Gefährdung der Sicherheit der Schweiz bestimmte Tätigkeiten verbieten zu können.

Die neue Bestimmung berührt die erwähnten Kompetenzen des Bundesrates nach den Artikeln 184 Absatz 3 und Artikel 185 Absatz 3 BV nicht. Sie bleiben parallel weiter bestehen (vgl. auch Kommentar zu den Artikeln 18e in fine und 29a Absatz 1).

Der Rechtsmittelweg verläuft bei Verboten oder Massnahmen, die vom Bundesrat kraft der Bundesverfassung verhängt werden, anders als bei einem Verbot durch das Departement gemäss der vorgeschlagenen Neuregelung. Die Entscheide des Bundesrates sind Regierungsakte; sie können nur dann vor einer Bundesgerichtsbarkeit gerügt werden, wenn das Völkerrecht einen Anspruch auf gerichtliche Beurteilung einräumt[4]. Ist dem nicht so, sind Entscheide des Bundesrates endgültig. Demgegenüber ist vorgesehen, dass gegen gestützt auf das BWIS ergangene Verfügungen die Beschwerde an das Bundesverwaltungsgericht möglich ist, dessen Entscheid an das Bundesgericht weiterziehbar ist.

Absatz 1
Mit dieser Bestimmung sollen bestimmte Tätigkeiten verboten werden können. So gibt es Handlungsweisen, die auf den ersten Blick harmlos oder gar fördernswert scheinen wie beispielsweise Geldsammlungen für einen in einem ausländischen Krisengebiet gelegenen Witwen- und Waisenfonds. Nicht selten gelangen dabei aber einerseits erpressungsähnliche Druckmassnahmen zur Anwendung (zum Beispiel werden die Mitglieder der hier ansässigen Diaspora direkt auf im Heimatland verbliebene Familienangehörige angesprochen und diesen für den Fall einer verweigerten Spende sinngemäss Benachteiligungen in Aussicht gestellt). Anderseits werden die so gesammelten Gelder aller Wahrscheinlichkeit nach nicht dem in der Schweiz für die Sammlung vorgeschobenen, sondern mindestens teilweise einem ganz anderen Zweck zugeführt, wie beispielsweise dem Kauf von Waffen für eine im Krisengebiet aktive Widerstandsbewegung. Für solche Machenschaften lässt sich indessen oft kaum direkter Beweis erbringen: Die in der Schweiz zu Spenden genötigten Personen schweigen aus Angst um sich und ihre im Heimatland verbliebenen Familienangehörigen, Freunde und Bekannte. Die Spur des Geldes

[4] Vgl. BGE 125 II 417 ff.; Diese Rechtsprechung wird ausdrücklich im Art. 83 Bst. a des Bundgerichtsgesetzes, BBl 2005 4093, und im Art. 32 Abs. 1 Bst. a des Bundesgesetzes über das Bundesverwaltungsgericht, BBl FF 2005 4093, verankert. Diese Gesetze werden voraussichtlich am 1. Januar 2007 rechtskräftig.

verliert sich in verschlungenen Geldtransfers, in mangelnden, gefälschten oder gegen Bezahlung echten, aber inhaltlich falschen ausländischen Bescheinigungen über die Verwendung des Geldes und so fort.

Der Departementsvorsteher oder die Departementsvorsteherin muss Umfang und Inhalt des Verbotes so genau wie möglich umschreiben. Die rechtlichen Sanktionen gegen einen Verbotsverstoss sind in Artikel 292 des Strafgesetzbuches geregelt. Ein gesetzlicher Verweis auf die strafrechtliche Norm erübrigt sich, da ihm bloss deklaratorischer Charakter zukäme.

Absatz 2
Angesichts der Auswirkung, die diese Verbote auf die Geltendmachung der Grundrechte Betroffener haben können, ist es wichtig, das sie befristet werden. So müssen die Behörden nach Ablauf der Gültigkeit eines Verbots erneut prüfen, ob die Bedingungen, unter denen ein Verbot verhängt werden kann, noch immer erfüllt sind.

Gegebenenfalls kann die Gültigkeitsdauer eines Verbots so lange verlängert werden, wie es die Umstände erfordern. Die hier angesprochene Befristung dient nicht demselben Zweck wie jene in Bezug auf die Bestimmungen in den Artikeln 184 Absatz 3 und 185 Absatz 3 BV. Die in der Bundesverfassung angesprochene Befristung soll gewährleisten, dass solche Massnahmen bei Fortbestand der Gefahr ins ordentliche Recht überführt werden müssen. Diese Befristung dient also in erster Linie dazu, dem Grundsatz der Gewaltentrennung und dem ordentlichen Gesetzgebungsverfahren Rechnung zu tragen. Die nun im BWIS vorgeschlagene Befristung hingegen rechtfertigt sich aus materiellen Gründen bzw. mit der Schwere des Grundrechseingriffs. Als Folge der Befristung wird das Departement ausdrücklich verpflichtet, regelmässig zu prüfen, ob die Anordnungsvoraussetzungen noch erfüllt sind, und allenfalls das Verbot umgehend aufzuheben. Das Departement ist also gehalten, nicht nur aktiv zu werden, um ein Verbot zu verhängen, sondern ebenso, wenn es darum geht, ein einmal verhängtes Verbot wieder aufzuheben.

Öffentliches Interesse und Verhältnismässigkeit
Das Verbot von Tätigkeiten ist ein schwerer Grundrechtseingriff und kann mehrere Grundrechte tangieren, soweit diese Grundrechte die entsprechenden Tätigkeiten schützen. So beispielsweise die Vereinigungsfreiheit (Art. 23, BV), die Glaubens- und Gewissensfreiheit (Art. 15 BV), die Meinungs- und Informationsfreiheit (Art. 16 BV), die Versammlungsfreiheit (Art. 22 BV) oder die Eigentumsgarantie (Art. 26 BV). Nach Artikel 36 BV müssen solche Beschränkungen vor allem durch ein öffentliches Interesse gerechtfertigt und verhältnismässig sein. Das öffentliche Interesse ergibt sich ohne weiteres aus der im Aufgabenbereich des BWIS verankerten Pflicht, frühzeitig Gefährdungen durch Terrorismus und gewalttätigen Extremismus zu erkennen und zu bekämpfen. In Bezug auf die Verhältnismässigkeit ist festzuhalten, dass das Verbot einer bestimmten Tätigkeit unter den im Gesetz genannten Bedingungen nicht a priori unverhältnismässig ist. Vielmehr ist die erforderliche Güterabwägung im konkreten Einzelfall vorzunehmen.

2.36 Artikel 27, Absatz 1bis
Artikel 27 des Gesetzes verpflichtet den Bundesrat, die eidgenössischen Räte, die Kantone und die Öffentlichkeit jährlich oder nach Bedarf über seine Beurteilung der Bedrohungslage und über die Tätigkeiten der Sicherheitsorgane des Bundes zu orientieren. Daran anknüpfend soll das Departement verpflichtet werden, jährlich

oder nach Bedarf über die Verwendung der mit vorliegender Revision neu eingeführten Mittel zu informieren. Angesichts der möglichen Beschränkung von Grundrechten der Bevölkerung versteht sich eine solche Berichterstattung von selbst. Es betrifft dies den Einsatz von Tarnidentitäten, der besonderen Mittel der Informationsbeschaffung sowie das Verbot von Tätigkeiten. Im Übrigen erfolgt bereits heute und ohne ausdrückliche gesetzliche Anordnung eine umfassende Berichterstattung an das Departement (im Rahmen der Berichterstattung über Operationen).

2.37 Artikel 29a
Das heutige BWIS enthält mit Ausnahme von Artikel 18 keine Bestimmungen über Verfahren und Rechtsschutz. Artikel 18 regelt das Auskunftsrecht über im Informationssystem des Bundesamtes bearbeitete Personendaten. Mit der Einführung der besonderen Mittel der Informationsbeschaffung entsteht Anpassungsbedarf an die Erfordernisse der Bundesverfassung und der Europäischen Menschenrechtskonvention (EMRK). Von besonderer Bedeutung sind dabei die Artikel 29a BV (Rechtsweggarantie) und Artikel 13 EMRK (Recht auf einen wirksamen Beschwerde); vgl. hierzu auch Kommentar zum Artikel 18j.

Absatz 1
Diese Bestimmung verankert das Beschwerderecht gegen Verfügungen im Sinne von Artikel 18i Absatz 1 und Artikel 18n. In beiden Fällen führt der Rechtsmittelweg an das Bundesverwaltungsgericht. Damit wird auch Artikel 32 Absatz 1 Buchstabe a des Bundesgesetzes über das Bundesverwaltungsgericht (VGG; BBl 2005 4093) präzisiert, indem klar festgelegt wird, dass die erwähnten Entscheide gemäss BWIS justiziable Verwaltungsverfügungen und nicht zur Kategorie der Regierungsakte gehören. Regierungsakte sind im Regelfall gerade nicht beim Bundesverwaltungsgericht anfechtbar (vgl. auch Kommentar zu Artikel 18n).

Weil im Falle von Artikel 18i Absatz 1 Anfechtungsgegenstand vor dem Bundesverwaltungsgericht die nachträgliche Mitteilung des Bundesamtes ist, hat die Zuweisung der Entscheidkompetenz für die Anordnung von besonderen Mitteln der Informationsbeschaffung an den Bundesrat keinen Einfluss auf das Beschwerdeverfahren.

Absatz 2
Bei Beschwerden gegen nach Artikel 18i Absatz 1 mitgeteilte besondere Mittel der Informationsbeschaffung rechtfertigen die Natur dieser Massnahmen, gleich wie die mit einer nachträglichen Rekonstruktion der Aktenlage einhergehenden Probleme, ein Abweichen von Artikel 49 des Bundesgesetzes über das Verwaltungsverfahren (VwVG; SR 172.021). In diesem Absatz wird die zulässige Rüge auf die Behauptung der Verletzung von Bundesrecht beschränkt. In den übrigen Fällen kann zusätzlich die unrichtige oder unvollständige Feststellung des rechtserheblichen Sachverhaltes und die Unangemessenheit gerügt werden (vgl. Artikel 49 Absatz 2 VwVG).

Absatz 3
Wie auch in anderen Bundesgesetzen üblich, wird für das Verfahren der Klarheit halber auf die allgemeinen Bestimmungen der Bundesrechtspflege verwiesen.

2.38 Bundesgesetz über das Bundesverwaltungsgericht[5]

Die Einführung von Artikel 13b BWIS bedingt die Anpassung des Bundesgesetzes über das Bundesverwaltungsgericht. Der Artikel legt nämlich fest, dass das Bundesverwaltungsgericht zuständig ist, Streitigkeiten zu schlichten zwischen dem Bundesamt und den Behörden, kantonalen Verwaltungseinheiten, den Organisationen, die öffentliche Aufgaben erfüllen, wie auch den Bundesorganen, die nicht der zentralen Bundesverwaltung angehören. (vgl. auch Kommentar zum Artikel 13b).

2.39 Schweizerisches Strafgesetzbuch[6], Artikel 179octies und Artikel 317bis

Art. 179^{octies}

Der Einsatz von technischen Überwachungsgeräten, wie Ton- und Bildaufzeichnungsgeräten im Geheimbereich, sind strafbare Handlungen im Sinne des Artikels 179 und folgende des Strafgesetzbuches. Der Artikel 179^{octies} behält indessen die amtliche Überwachung nach Massgabe des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vor.

Diese Strafbestimmung muss deshalb angepasst werden, damit auch die neuen, im Verfahren nach BWIS durchgeführten Überwachungsmassnahmen vorbehalten bleiben.

Art. 317bis

Urkundenfälschung ist eine strafbare Handlung (vgl. Artikel 251, 252, 255, 317, StGB). Der heutige Artikel 317bis StGB behält indessen die Herstellung und Verwendung gefälschter Urkunden vor, die zum Aufbau oder zur Aufrechterhaltung einer Legende im Rahmen einer richterlich genehmigten verdeckten Ermittlung verwendet werden. Diese Strafbestimmung muss angepasst werden, damit auch die Verwendung der Tarnidentitäten gemäss BWIS vorbehalten bleiben.

2.40 Bundesgesetz über die Armee und die Militärverwaltung[7], Artikel 99, Absatz 1, zweiter Satz; Absätze 1bis und 2 sowie Artikel 99a

Art. 99 Absatz 1, zweiter Satz, 1bis und 2

Absatz 1, zweiter Satz

Die in Artikel 99 Absatz 1 des Gesetzesentwurfs vorgesehene (grundsätzliche) Beschränkung der Funkaufklärung auf Ziele im Ausland soll die Empfehlung 1 der Geschäftsprüfungsdelegation aus deren Bericht vom 10. November 2003 zum Projekt ONYX umsetzen. Unter Funkaufklärung gegen Ziele im Ausland ist die Erfassung von elektromagnetischen Ausstrahlungen im Ausland zu verstehen. Heute geschieht dies mittels des Systems ONYX für den Bereich der Satellitenkommunikation oder mittels Kurzwellenempfangsanlagen für dieses Frequenzspektrum. Welche Mittel und Systeme in Zukunft für einen auf das Ausland bezogenen Funkaufklärungsauftrag eingesetzt werden, wird eine Frage der technischen Entwicklung sein. Der Gesetzestext lässt dies mit der allgemeinen Formulierung "Funkaufklärung" bewusst offen.

Absatz 1bis

Die Funkaufklärung soll nach Absatz 1 Satz 2 grundsätzlich gegen Ziele im Ausland eingesetzt werden. Es gibt jedoch weiterhin Funkaufklärungsbedürfnisse der Armee

[5] AS ... (BBL 2005 4093)
[6] SR **311.0**
[7] SR **510.10**

im Inland. Angesichts des grundsätzlichen Charakters der Regel von Absatz 1 Satz 2 und des Umstandes, dass Einschränkungen der Grundrechte wie desjenigen auf der Wahrung der Privatsphäre einer formellgesetzlichen Grundlage bedürfen, muss der Einsatz der Funkaufklärung im Inland gegen Zivilpersonen explizit geregelt werden. Absatz 1bis sieht deshalb die folgenden beiden Fälle vor, bei denen die Funkaufklärung der Armee im Inland gegen Zivilpersonen gestattet ist:

Buchstabe a bezieht sich auf die Frequenzüberwachung. Die Armee soll bei ihren Einsätzen die ihr zugewiesenen militärischen Frequenzen auf allfällige zivile Nutzer überprüfen können. Gegebenenfalls wird sie diese zivilen Frequenznutzer identifizieren und ausfiltern. Nur durch die Elimination von unerwünschten zivilen Nutzern kann die Armee die für die Auftragserfüllung notwendige Kommunikationsfähigkeit sicherstellen.

Buchstabe b bezieht sich auf die Wahrung der Lufthoheit. Die Luftwaffe hat nach der Verordnung vom 23. März 2005 über die Wahrung der Lufthoheit (VWL, SR 748.111.1) die Lufthoheit sicherzustellen. Sie muss zu diesem Zweck mittels Funkaufklärung den Funkverkehr zwischen militärischen und zivilen Flugzeugen und ihren (zivilen oder militärischen) Bodenstationen erfassen können. Auf diese Weise können u.a. unbekannte Flugobjekte erkannt, identifiziert und gegebenenfalls die richtigen Abwehrmittel ergriffen werden. Die Funkaufklärung dient der Luftwaffe auch zur generellen Überwachung des Luftraums und zur Darstellung der Luftlage, wozu sie nach Artikel 5 VWL verpflichtet ist.

Des Weiteren ist der Einsatz der Funkaufklärung durch die Armee gegen zivile Ziele im Inland (oder im Ausland) auch dann gestattet, wenn er im Rahmen der Notwehr oder des Notstandes erfolgt, zum Beispiel um Armeeangehörige vor einem bevorstehenden Angriff durch Zivilpersonen zu schützen. Es handelt sich hier um einen klassischen Rechtfertigungsgrund, der im Militärgesetz nicht explizit vorgesehen werden muss, da er in den Artikeln 25 und 26 des Militärstrafgesetzes (MStG, RS 321) bereits hinlänglich geregelt ist.

Artikel 99a

In Übereinstimmung mit Artikel 164 Absatz 1 BV müssen alle wichtigen rechtsetzenden Normen in Form eines formellen Gesetzes erlassen werden. Die heutigen Bestimmungen zur Funkaufklärung in der Verordnung über die elektronische Kriegsführung enthalten rechtsetzende Normen, haben aber keine ausdrückliche formellgesetzliche Grundlage im Militärgesetz. Es gilt deshalb, für diese Bestimmungen eine angemessene Rechtsgrundlage zu schaffen.

Absatz 1

Mit dieser Bestimmung wird die heutige »Unabhängige Kontrollinstanz« (UKI) auf Gesetzesebene verankert. Derzeit dienen die Bestimmungen in Artikel 14 ff. der Verordnung vom 15. Oktober 2003 über die elektronische Kriegsführung (VEKF, RS 510.292) als Rechtsgrundlage dieser Instanz.

Die unabhängige Kontrollinstanz kontrolliert grundsätzlich nur Funkaufklärungsaufträge, für die keine besondere (Einzel-) Bewilligung auf politischer Stufe vorgesehen ist, wie dies bei den Aufträgen (z.B. des Strategischen Nachrichtendienstes des VBS) für die ständige Funkaufklärung der Fall ist. Funkaufklärung im Ausland (durch die Armee) kann aber auch im Rahmen eines

Friedensförderungsdienstes stattfinden. Hier schliesst der entsprechende Parlamentsbeschluss die Bewilligung für die Funkaufklärung mit ein. Weil in diesen Fällen eine Bewilligung der zuständigen politischen Behörde vorliegt, erfolgt keine zusätzliche Überprüfung des Funkaufklärungsauftrages durch die unabhängige Aufsichtsbehörde.

Die Instanz kontrolliert die Rechtmässigkeit der ständigen Funkaufklärung, was auch die Kontrolle der Verhältnismässigkeit der Massnahme impliziert. Die Instanz spricht sich indessen nicht zur Zweckmässigkeit der Kontrolle aus.

Damit ihre Unabhängigkeit gewährt ist, verrichtet die Instanz ihre Aufgaben weisungsunabhängig.

Absatz 2
Diese Bestimmung delegiert die Regelung der Zusammensetzung dieser Behörde an den Bundesrat.

2.41 Fernmeldegesetz[8], Artikel 44
Artikel 44 FMG muss ergänzt werden, da neu für die Überwachung des Fernmeldeverkehrs nicht mehr nur das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs gilt (BÜPF, SR 780.1), sondern auch das Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (SR 120).

Die auf das BÜPF gestützte Überwachung des Post- und Fernmeldeverkehrs erfolgt im Rahmen eines Strafverfahrens des Bundes oder eines Kantons oder zum Vollzug eines Rechtshilfeersuchens nach dem Rechtshilfegesetz vom 20. März 1981 (SR 351.1). Eine Überwachung des Post- und Fernmeldeverkehrs gestützt auf das BWIS wird zum Zwecke der Erkennung von Gefährdungen durch Terrorismus, verbotenen politischen oder militärischen Nachrichtendienst und verbotenen Handel mit Waffen, radioaktiven Materialien und verbotener Technologie durchgeführt.

[8] SR **784.10**

3. Auswirkungen

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen
Die finanziellen Auswirkungen sind abhängig von Art und Ausgestaltung der einzelnen Massnahmen und von deren Nutzung.

3.1.2 Personelle Auswirkungen
Für die Umsetzung der Massnahmen soll weitestgehend auf die bestehenden eidgenössischen (Bundesverwaltungsgericht, Dienst für Analyse und Prävention) und kantonalen Strukturen (kantonale Nachrichtendienste) aufgebaut werden. Für Bundesverwaltungsgericht, Dienst für besondere Aufgaben UVEK (für die Post und Fernmeldeüberwachungen) und die rechtliche, operationelle und administrative Umsetzung der neuen Beschaffungsmöglichkeiten sowie Verarbeitung der Resultate bei fedpol ist mit insgesamt rund 40 Stellen zu rechnen. Diese sollen durch EJPD-interne Kompensationen geschaffen werden.

Dabei ist der Stellenmehrbedarf schwergewichtig auf folgende Bereiche zurückzuführen:
- Stärkung der operationellen Strukturen, insbesondere der mit der Informationsbeschaffung und –bearbeitung befassten polizeilichen Stellen (Polizisten, Dolmetscher, Techniker, operative Analytiker);
- Stärkung der datenverarbeitenden Strukturen, insbesondere der Datenerfassung, der Qualitätssicherung und beim Verkehr mit dem Ausland;
- Stärkung Nachrichtendienst-fremder Strukturen wie des DBA UVEK (Technik und Administration) oder des Bundesverwaltungsgerichts (Sekretariat).

Folglich können die zusätzlichen Kompetenzen weiterhin mit einem engen Ressourcenansatz umgesetzt werden.

3.1.3 Sonstige Auswirkungen
Die sonstigen Auswirkungen sind abhängig von Art und Ausgestaltung der einzelnen Massnahmen.

3.2 Auswirkungen auf Kantone und Gemeinden
Das Sicherheitsniveau in den Kantonen und Gemeinden steigt. Allenfalls marginal erhöhten Auskunfts- und Meldepflichten stehen mittel- bis langfristig Entlastungen (erleichterte Abklärungen, teilweise Ablösung der personalaufwändigen und entsprechend teuren Observationen durch die besonderen Mittel der Informationsbeschaffung usw.) gegenüber, welche sich zum heutigen Zeitpunkt noch nicht beziffern lassen. Abhängig von der Art und Ausgestaltung der neuen Massnahmen ist denkbar, dass in den Kantonen zusätzliches Arbeitsvolumen entsteht. Je nach Betroffenheit werden die Kantone deshalb über zusätzliche personelle Mittel zu befinden haben.

3.3 Auswirkungen auf die Volkswirtschaft

Nach den Richtlinien des Bundesrates vom 15. September 1999 für die Darstellung der volkswirtschaftlichen Auswirkungen von Vorlagen des Bundes (BBl 2000 1038) ist eine Vorlage nach folgenden Punkten zu prüfen:

3.3.1 Notwendigkeit und Möglichkeit staatlichen Handelns

Die Vorlage dient u.a. der Umsetzung politischer Vorstösse. Der Bundesrat beauftragte das EJPD, die nötigen Entwürfe für Gesetzesrevisionen zu unterbreiten. Im Übrigen ist die Zuständigkeit des Bundes gegeben.

3.3.2 Auswirkungen auf die einzelnen gesellschaftlichen Gruppen

Die vorgeschlagenen Normen führen zu einer Stärkung der inneren Sicherheit und damit zu einer Verbesserung des Schutzes der Bevölkerung.

3.3.3 Auswirkungen auf die Gesamtwirtschaft

Es sind keine direkten Auswirkungen auf die Gesamtwirtschaft ersichtlich. Indirekt werden durch ein sicheres Umfeld die Rahmenbedingungen verbessert.

3.3.4 Alternative Regelungen

Für die innere Sicherheit seines Gebietes ist in erster Linie der Kanton verantwortlich. Soweit der Bund nach Verfassung und Gesetz für die innere Sicherheit verantwortlich ist, leisten ihm die Kantone Amts- und Vollzugshilfe. Nach geltendem Recht ist der Bund insbesondere zuständig zur frühzeitigen Erkennung von Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus, verbotenen Handel mit Waffen und radioaktiven Materialien sowie verbotenem Technologietransfer (Nonproliferation). Er unterstützt die zuständigen Polizei- und Strafverfolgungsbehörden durch Mitteilung von Erkenntnissen über das organisierte Verbrechen. Der Bund legiferiert somit in seinem Kompetenzbereich; Raum für alternative Regelungen besteht keiner.

3.3.5 Zweckmässigkeit im Vollzug

Die Umsetzung der Vorlage erfolgt auf der Grundlage der bewährten bisherigen Strukturen der Sicherheitsbehörden. Am Gesamtkonzept der gemeinsamen Verantwortung von Bund und Kantonen für den Staatsschutz ändert sich nichts.

3.4 Andere Auswirkungen

3.4.1 Auswirkungen auf die internationalen Beziehungen

Die Gesetzesrevison setzt formal keine direkten internationalen Verpflichtungen um. Die Angleichung der Standards führt zu einer deutlichen Verbesserung der internationalen Zusammenarbeit.

3.4.2 Auswirkungen auf das Ansehen der Schweiz

Das internationale Ansehen der Schweiz erfährt eine nachhaltige Steigerung, insbesondere was ihren Willen zur wirkungsvollen Bekämpfung des internationalen Terrorismus betrifft.

4. Rechtliche Aspekte

4.1 Verfassungsgrundlage

Das BWIS stützt sich auf die ungeschriebene Bundeskompetenz zur Wahrung der inneren und äusseren Sicherheit der Eidgenossenschaft. In diesem Rahmen bewegt sich auch die vorliegende Gesetzesrevision. Sie überschreitet den in Artikel 2 Absatz 1 und 2 BWIS verankerten Aufgabenbereich nicht. Sie unterschreitet ihn, soweit sich der Anwendungsbereich einzelner Massnahmen auf Terrorismus, verbotenen militärischen und politischen Nachrichtendienst und Handel mit Waffen und radioaktiven Materialien sowie verbotenen Technologietransfer beschränkt. Weder gewalttätiger Extremismus, noch verbotener wirtschaftlicher Nachrichtendienst oder organisierte Kriminalität bilden Gegenstand vorliegender Gesetzesrevision.

4.2 Vereinbarkeit mit den Grundrechten

Die im Rahmen der vorliegenden Revision vorgeschlagenen Massnahmen können in Grundrechte eingreifen. Tangiert werden können insbesondere die Privatsphäre (Artikel 13 BV), die Vereinigungsfreiheit (Artikel 23 BV), die Glaubens- und Gewissensfreiheit (Artikel 15 Absatz 3), die Versammlungsfreiheit (Artikel 22) und die Eigentumsgarantie (Artikel 26).

Nach dem Wortlaut von Artikel 36 BV bedürfen Einschränkungen von Grundrechten einer gesetzlichen Grundlage, müssen durch ein öffentliches Interesse oder durch den Schutz der Grundrechte Dritter gerechtfertigt sein und den Grundsatz der Verhältnismässigkeit wahren. Zudem darf der Kern der Grundrechte nicht verletzt werden. Einschränkungen eines Gundrechtes sind zulässig sofern konkrete Rechtsgüter Dritter oder der Allgemeinheit in schwerwiegender Weise gefährdet oder verletzt werden.

Die vorgeschlagenen Mittel und Massnahmen basieren auf einem Gesetz im formellen Sinn, dem BWIS. Das öffentliche Interesse besteht im Schutz der inneren oder äusseren Sicherheit sowie in der frühzeitigen Erkennung von Gefährdung, namentlich durch Terrorismus, verbotenen politischen und militärischen Nachrichtendienst, verbotenen Handel mit Waffen und radioaktiven Materialien und verbotenen Technologietransfer. Zweifelsohne ist ein legitimes öffentliches Interesse vorhanden. Für die Prüfung der Verhältnismässigkeit der neuen Massnahmen wird auf die Erläuterungen zu den einzelnen Gesetzesartikeln verwiesen (so insbesondere zu den Artikeln 13a, 13c, 13d, 18k, 18l, 18m, 18n). In diesem Zusammenhang ist auch in Erinnerung zu rufen, dass es bei der Prüfung der Verhältnismässigkeit des staatlichen Eingriffs die mit den jeweiligen Massnahmen einhergehenden Begleitumstände mit zu berücksichtigen gilt (so insbesondere die als ultima ratio ausgestalteten Anordnungsvoraussetzungen, das Anordnungsverfahren mit vorgängiger Prüfung der juristischen und politischen Voraussetzungen, der garantierte Zugang zu einer richterlichen Prüfung usw.). Im Übrigen ergibt sich aus den Anordnungsvoraussetzungen nach Artikel 18b, insbesondere Buchstaben c, unmissverständlich die subsidiäre Natur von Massnahmen mit Grundrechtseingriffen. Sie sollen mit anderen Worten nur zur Anwendung gelangen, wenn sich andere Informationsbeschaffungsmassnahmen für die Abklärung eines konkreten Verdachts einer Gefährdung der inneren oder äusseren Sicherheit der Schweiz als unzureichend erweisen („ultima ratio“).

Das BWIS dient der Stärkung der Sicherheit der Schweiz und seiner Einwohner. Die einzelnen Mittel und Massnahmen der Vorlage sind verfassungskonform,

4.3 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Als Vertragspartei verschiedener internationaler Menschenrechtsverträge und Konventionen obliegt es der Schweiz, den internationalen Kontrollorganen regelmässig über die Umsetzung ihrer völkerrechtlichen Verpflichtungen Bericht zu erstatten. Auch unter diesem Aspekt leistet die Verabschiedung der hier vorgeschlagenen Mitteln und Massnahmen einen wichtigen Beitrag zum Kampf gegen Terrorismus und weitere gravierende Gefährdungen der internationalen Sicherheit, was dem Ansehen der Schweiz im internationalen Umfeld förderlich ist.

Der vorliegende Gesetzesentwurf steht sowohl in Bezug auf seine allgemeine Zielrichtung wie auch hinsichtlich der einzelnen Bestimmungen im Einklang mit der EMRK und dem Internationalen Pakt über bürgerliche und politische Recht (Pakt II; SR 0.103.2).

Gemäss EMRK kann die Ausübung grundlegender Rechte (wie beispielsweise die Achtung des Privat- und Familienlebens nach Artikel 8 oder die Versammlungsfreiheit nach Artikel 11 EMRK) eingeschränkt werden, wenn die Einschränkung gesetzlich vorgesehen ist, ein legitimes Ziel verfolgt und in einer demokratischen Gesellschaft notwendig sind. Das vorliegende Revisionspaket erfüllt die Voraussetzungen an ein Gesetz im materiellen Sinne gemäss EMRK. Insbesondere legen die neuen Bestimmungen den betroffenen Personenkreis (vgl. insbesondere Artikel 18k bis 18n), die Anwendungsvoraussetzungen (vgl. insbesondere Artikel 18a und 18b) und die Verfahrensgarantien (vgl. insbesondere Artikel 18c, 18d und 18i) mit hinreichender Bestimmtheit fest. Die Prüfung der zwei übrigen Voraussetzungen (legitimes Ziel, Notwendigkeit in einer demokratischen Gesellschaft) entspricht derjenigen des öffentlichen Interesses und der Verhältnismässigkeit (vgl. oben).

Der UNO Pakt II garantiert in Bezug auf die vorliegend zur Diskussion stehenden Grundrechte (vgl. Art. 17 bzw. Art. 22 Pakt II) keinen weitergehenden Schutz als die EMRK oder die BV.

Im Übrigen sind die vorgeschlagenen Mittel mit den spezifisch auf Terrorismus zugeschnittenen Abkommen und Vereinbarungen ohne weiteres kompatibel.

Anhang 1

Hängige Gesetzgebungsprojekte im Bereich der inneren Sicherheit

Internationale Vereinbarungen

Titel	**Inhalt**	**Geschäftsstand**	**Relevante Schnittstellen mit vorliegender Revision**
Bilaterale Abkommen zur Durchführung von Schengen	Bilaterale Abkommen zur Durchführung des Schengener Acquis	Prüfung der Notwendigkeit	Nein
Europol: Absichtserklärung für eine Ausweitung des Mandats und eine Änderung der Klassifizierungs-vorschriften	Ausweitung des Anwendungsbereichs von Europol auf neue Delikte	Entwurf	Nein
Europol: Stationierungsabkommen mit den Niederlanden	Stationierung von Schweizer Attachés in den Niederlanden	Entwurf	Nein
Absichtserklärung CH-BRD betr. WM06 (Memorandum of understanding)	Zusammenarbeit im Rahmen der WM 2006	Unterzeichnung im Mai 2006	Nein
Abkommen mit Slowenien über die grenzüberschreitende Polizeizusammenarbeit	Bilaterale Polizeizusammenarbeit	Beratung im Ständerat	Nein
Abkommen mit Lettland / Tschechien über die grenzüberschreitende Polizeizusammenarbeit	Bilaterale Polizeizusammenarbeit	Beratung im Nationalrat	Nein
Abkommen mit Albanien / Mazedonien / Rumänien über die grenzüberschreitende Polizeizusammenarbeit bzw. Anpassung Staatsvertrag mit Frankreich / Italien bzw. Zusammenarbeit mit Liechtenstein bzw. Staatsvertrag mit Bosnien-Herzegowina / Lettland / Montenegro / Serbien / Slowenien / Tschechien / Türkei / Ukraine / USA	Bilaterale Polizeizusammenarbeit	Aussprachepapier zur Strategie zur internationalen Polizeikooperation beim Bundesrat	Nein

Gesetze

Titel	Inhalt	Geschäftsstand	Relevante Schnittstellen mit vorliegender Revision
Schweizerische Strafprozessordnung	Vereinheitlichung des Schweizerischen Strafprozessrechts	Botschaft	Regelung der polizeilichen Vorabklärungen und der Weitergabe von Informationen aus Strafverfahren
Polizeigesetz	Schaffung der Rechtsgrundlagen für Bundesorgane mit polizeilichen Aufgaben	Vorprojekt	Ev. später Transfer des BWIS in PolG
Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS I)	Präventive Bekämpfung von Gewalt, namentlich an Sportveranstaltungen	Vom Parlament verabschiedet; Inkrafttreten noch offen	Ja (Gliederung Gesetz)
Bundesgesetz über Waffen, Waffenzubehör und Munition (Waffengesetz)	Verbesserung der Missbrauchsprävention bzw. Anpassung an Schengen	In Kommission Ständerat	Nein
Bundesgesetz über polizeiliche Informationssysteme des Bundes	Vereinheitlichung der formellgesetzlichen Grundlagen für die vom Bund geführten polizeilichen Informationssysteme	Auswertung Vernehmlassung	Nein
Bundesgesetz über die Anwendung von Zwang im Ausländerrecht und beim Transport von Personen im Auftrag der Bundesbehörden	Einheitliche Rahmenbedingungen für den Einsatz körperlicher Gewalt, den Einsatz von Hilfsmitteln wie Fesseln sowie den Einsatz von Waffen	Botschaft	Nein
Bundesgesetz über Massnahmen gegen Rassismus	Verbot rassistischer Embleme bzw. Zulässigkeit von Kommunikations-überwachung im Rahmen eines Strafverfahrens nach Art. 261bis StGB	Auswertung Vernehmlassung	Nein

Verordnungen

Titel	**Inhalt**	**Geschäftsstand**	**Relevante Schnittstellen mit vorliegender Revision**
Verordnung über Massnahmen zur Wahrung der inneren Sicherheit	Vollzug BWIS I	Entwurf	Nein
Verordnung über das Staatsschutz-Informations-System	Regelung des Datenaustausches mit Europol	Auswertung Ämterkonsultation	Nein
SIRENE-Verordnung	Regelung der Aufgaben des SIRENE-Büros	Entwurf	Nein
Verordnung über das Informationssystem der Bundeskriminalpolizei	Anpassung an Europol	Auswertung Ämterkonsultation	Nein
Verordnung über Waffen, Waffenzubehör und Munition	Anpassung an Gesetzesrevision	Entwurf	Nein
SIS-Verordnung	Vollzug von Art. 351^{decies} StGB sowie Regelung Datenbearbeitung	Entwurf	Nein
Verordnung über die Aus-, Ein- und Durchfuhr zivil und militärisch verwendbarer Güter sowie besonderer militärischer Güter	Anpassung an Schengen	Entwurf	Nein
Verordnung über das Kriegsmaterial	Anpassung an Gesetzesrevision	Entwurf	Nein
Verordnung über Einreise und Anmeldung von Ausländerinnen und Ausländern	Anpassung an Schengen	Entwurf	Meldeformular ähnlich den bisherigen „Hotelmelde-scheine“
Verordnung über die Bearbeitung erkennungsdienstlicher Daten	Anpassung an Dublin (Eurodac)	Entwurf	Nein
Verordnung über das informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei	Anpassung an Europol	Entwurf	Nein

Anhang 2

Rechtsvergleich (Deutschland, Österreich, Frankreich, Italien, Luxemburg, Niederlande, EU)

1. Deutschland

Die Bundesrepublik Deutschland ist ein Bundesstaat und föderalistisch organisiert. Die föderale Verfassungsordnung Deutschlands weist den Ländern grundsätzlich die Polizeihoheit auf ihrem jeweiligen Staatsgebiet zu. Gleichzeitig sieht das Grundgesetz aber in zentralen Bereichen des Polizeiwesens originäre Zuständigkeiten des Bundes vor. Dies betrifft insbesondere die Regelung der Zusammenarbeit von Bund und Ländern in kriminalpolizeilichen Angelegenheiten sowie die gesamte internationale Verbrechensbekämpfung. Darüber hinaus gewährleistet der Bund die Sicherheit an den Landesgrenzen wie auch im Bahn- und Luftverkehr. Er erlässt zur Erfüllung seiner Aufgaben eigene Gesetze und führt Polizeibehörden in eigener Verantwortung. Aufgrund dieser Kompetenzverteilung gibt es in Deutschland außer den 16 Länderpolizeien die Polizeibehörden des Bundes. Diese sind das Bundeskriminalamt und die Bundespolizei. Beide gehören zum Geschäftsbereich des Bundesministeriums des Innern.
Hauptaufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen über die Bestrebungen, welche sich gegen die freiheitliche demokratische Grundordnung richten, sowie sicherheitsgefährdende oder geheimdienstliche Tätigkeiten und Bestrebungen im Geltungsbereich des Bundesverfassungsschutzgesetztes.[9]
Der Bund und die Länder sind in Angelegenheiten des Verfassungsschutzes zur Zusammenarbeit verpflichtet. Der Bund unterhält ein Bundesamt für Verfassungsschutz (BfV), welches dem Bundesminister des Innern untersteht. Das BfV darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschliesslich personenbezogener Daten verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen im BVerfSchG entgegenstehen. Zusätzlich kann es Daten und Informationen von den repressiven Behörden beziehen.[10] Umgekehrt darf der Bundesnachrichtendienst Informationen an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner aufgaben erforderlich ist oder wenn die Daten für Zwecke der öffentlichen Sicherheit benötigt werden.[11] Diese Daten dürfen für Strafverfolgungszwecke verwendet werden.
Im Dezember 2004 hat das neue Terrorismusabwehrzentrum seine Arbeit aufgenommen. In diesem Zentrum werden der Bundesnachrichtendienst, die Kriminal- und Verfassungsschutzämter der Länder, der Bundesgrenzschutz, das

[9] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz; BVerfSchG)
[10] § 18 BVerfSchG
[11] § 9 Gesetz über den Bundesnachrichtendienst vom 20. Dezember 1990 (BNDG)

Zollkriminalamt und der Militärische Abschirmdienst (MAD) in die Arbeitsläufe eingebunden.
Die Tätigkeiten des BfV unterliegen der Kontrolle durch ein Parlamentarisches Kontrollgremium, welches regelmässig über die allgemeine Tätigkeit des BfV und über Vorgänge von besonderer Bedeutung zu unterrichten ist.[12] Die Bundesregierung hat dem Parlamentarischen Kontrollgremium auf Verlangen Einsicht in den Akten und Dateien zu geben und die Anhörung von Mitarbeitern zu gestatten. Das BfV ist verpflichtet, Betroffenen auf Antrag unentgeltlich Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt.[13] Die gespeicherten Daten müssen berichtigt werden, sofern sie unrichtig sind. Spätestens nach fünf Jahren muss das BfV bei der Einzelfallbearbeitung prüfen, ob die Daten zu berichtigen oder zu löschen sind. Spätestens 15 Jahre nach dem Zeitpunkt der letzten Speicherung sind die Informationen zu löschen, ausser bei abweichender Entscheidung der Behördenleiter.[14]
Nachfolgend werden lediglich die Bestimmungen des Bundes erläutert.
Im Einzelfall darf das BfV zur Erfüllung seiner Aufgaben u. a. Telekommunikationsdaten und Teledienstleistungen einholen[15]. Der Antrag ist durch den Präsidenten des BfV oder seinen Vertreter schriftlich zu stellen und zu begründen. Über den Antrag entscheidet das vom Bundeskanzler beauftragte Bundesministerium. Dieses unterrichtet monatlich die G 10- Kommission über die beschiedenen Anträge vor deren Vollzug. Bei Gefahr in Verzuge kann das Bundesministerium den Vollzug der Entscheidung auch bereits vor der Unterrichtung der Kommission anordnen.[16] Das zuständige Bundesministerium unterrichtet im Abstand von höchstens sechs Monaten das Parlamentarische Kontrollgremium (PKGr) über die Durchführung der Informationsbeschaffungen. Weiter ist das BfV zum Einsatz von Vertrauensleuten und Gewährspersonen befugt sowie Observationen, Bild -und Tonaufzeichnungen (Grosser Lauschangriff), Tarnpapiere und Tarnkennzeichen anzuwenden.[17] Diese Massnahmen sind in einer Dienstvorschrift zu benennen, welche wiederum der Zustimmung des Bundesministers des Innern bedarf. Dieses unterrichtet das parlamentarische Kontrollgremium. Werden Auskünfte beim Betroffenen eingeholt, so muss der Erhebungszweck angegeben werden.
Das BfV ist des Weiteren unter bestimmten Voraussetzungen befugt, Auskünfte bei Banken einzuholen.[18] Auch darf das BfV, wenn es Informationen über Kommunikationswege terroristischer Gruppen benötigt, von den Erbringern von Postdienstleistungen Auskünfte wie z. B. Namen, Adressen und Angaben zu Postfächern einholen sowie Telekommunikationsverbindungsdaten wie Kennungen, Rufnummern und Daten über Standorte.[19] Schliesslich darf das BfV IMSI-Catchers zur Ermittlung der Geräte- und Kartennummern von mobilen Telefonen einsetzen.[20] Es gelten dabei die gleichen Voraussetzungen wie bei den Telefonabhörungen.

[12] § 2 Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes
[13] § 15 BVerfSchG
[14] § 12 BVerfSchG
[15] § 8 Abs. 8 BVerfSchG.
[16] § 8 Abs. 9 BVerfSchG
[17] § 8 Abs. 2 BVerfSchG
[18] § 8 Abs. 5 BVerfSchG
[19] § 8 Abs. 6 BVerfSchG und § 8 Abs. 8 BVerfschG
[20] § 9 Abs. 4 BVerfSchG

Dagegen stehen den Verfassungsschutzbehörden Deutschlands keinerlei polizeiliche Befugnisse zu, namentlich dürfen keine Durchsuchungen durchgeführt und keine Gegenstände beschlagnahmt werden.

2. Österreich

Das österreichische Staatssystem ist föderalistisch organisiert. Ihre Rechtsordnung macht grundsätzlich einen Unterschied zwischen dem repressivem und dem präventiven Bereich. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) nimmt die Tätigkeit des zivilen Nachrichtendiensts Österreich wahr.[21] Die Aufgaben des BVT sind im Wesentlichen der Schutz des Staates und seiner verfassungsmässigen Einrichtungen. Zu seinen Kernaufgaben zählen die Bekämpfung des internationalen Terrorismus, extremistischer Phänomene, der Spionage, des internationalen Waffenhandels, des Handels mit Kernmaterial und der organisierten Kriminalität in diesen Bereichen. Das BVT ist Teil der Generaldirektion für die öffentliche Sicherheit im Bundesministerium für Inneres. Das BVT besteht aus einem Leitungsbereich und aus drei Abteilungen. Die Abteilung 1 ist verantwortlich für Personalangelegenheiten, Schulung, Budget und Wirtschaftsahngelegenheiten. Zusätzlich werden hier u. a. alle rechtlichen Grundsatzahngelegenheiten im Staatsschutzbereich behandelt.
Die größte Organisationseinheit des BVT stellt die 2. Abteilung (Informationsbeschaffung, Analyse und Ermittlung) dar. Sie besteht aus fünf Referaten (Extremismus, Terrorismus und Ausländerextremismus, Spionageabwehr, Proliferation und Waffenhandel, Strategische Analyse sowie die operative Unterstützung) und koordiniert die 9 Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) bundesweit in Staatsschutzangelegenheiten.
Durch die 3. Abteilung werden bundesweit die Personen- und Objektschutzmaßnahmen veranlasst und koordiniert sowie die ausgearbeiteten Sicherheitsmaßnahmen laufend im Hinblick auf mögliche Bedrohungssituationen evaluiert. Im Weiteren werden hier Sicherheitsüberprüfungen durchgeführt.

Jedes Bundesland verfügt für die Aufgabenerfüllung im Bereich Verfassungsschutz über ein Landesamt für Verfassungsschutz und Terrorismusbekämpfung, welches Teil der jeweiligen Sicherheitsdirektion ist. Darüber hinaus obliegt dem BVT die Veranlassung und Koordination und via der LVT auch die Umsetzung von Personen- und Objektschutzmassnahmen sowie der Schutz von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte.
Den Staatsschutzbehörden ist der Zugriff auf Daten der repressiven Behörden gestattet. Letztere liefern ihre Informationen an die Staatsschutzbehörden weiter. Die Betroffenen haben das Recht auf Auskunft, Richtigstellung oder Löschung personenbezogener Daten und Möglichkeit der Beschwerde an die Datenschutzkommission. Wenn Staatsschutzinteressen es erfordern, kann ausnahmsweise die Auskunft verweigert werden.
Die Sicherheitsbehörden, welche die erweiterte Gefahrenerforschung ausüben, haben unverzüglich den Bundesminister für Inneres über die von ihnen ergriffenen Massnahmen zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Mitsprache zu geben, sofern er ein entsprechendes Begehren gestellt hat.

[21] Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei vom 31. Oktober 1992 (Sicherheitspolizeigesetz; SPG)

Nimmt der Rechtsschutzbeauftragte wahr, dass durch das Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenanwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus Gründen nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzkommission befugt
Über die Tätigkeiten im Rahmen der erweiterten Gefahrenerforschung (Beobachtung von Gruppierungen) hat der Rechtsschutzbeauftragte dem Bundesminister für Inneres jährlich zu berichten[22]. Dieser hat den Bericht dem ständigen Unterausschuss des Nationalrates auf dessen Verlangen zugänglich zu machen.

Die Staatsschutzbehörden sind ermächtigt, von den Betreibern öffentlicher Telekommunikationsdienste unter bestimmten Voraussetzungen Auskünfte einzuholen. Die Post- und Fernmeldeüberwachung ist jedoch nur den repressiven Behörden gestattet. Auch kann verdeckt ermittelt und dabei eine Tonaufnahme hergestellt werden.[23] Die Tonaufnahme ohne gleichzeitige Anwesenheit des verdeckten Ermittlers ist unzulässig. Dem Rechtsschutzbeauftragten obliegt die begleitende Kontrolle der verdeckten Ermittlung und des verdeckten Einsatzes von Bild- und Tonaufzeichnungsgeräten. Über solche Ermittlungen ist der Rechtsschutzbeauftragte mit Angabe der für die Ermittlungen wesentlichen Gründe in Kenntnis zu setzen, soweit die Identität der Betroffenen bekannt ist. Den Staatsschutzbehörden ist des Weiteren die Sicherstellung, Beschlagnahmung, Einziehung[24] ,das Observieren[25] und Betreten von privaten Räumen[26] gestattet, sowie die Anordnung und Durchführung von Befragungen.[27] Finanzintermediäre sind in bestimmten Fällen verpflichtet, Auskünfte den zuständigen Behörden zu übermitteln.[28]

Die Tätigkeit des BTV unterliegt der parlamentarischen Kontrolle gemäss Art. 52 a B-VG. Nach Erschöpfung des administrativen Instanzenzuges kann beim Verwaltungs- oder Verfassungsgerichtshof Beschwerde erhoben werden.

Auch in Österreich blieb der 11. September 2001 nicht ohne Folgen. Die Strukturen sind gestrafft und die Gesetzesbestimmungen verschärft worden. Im Zuge dieser Verschärfung haben die Staatschutzbehörden weiter reichende Kompetenzen erhalten.
Durch die Sicherheitspolizeigesetz-Novelle 2002 erfolgte eine Ausdehnung des Schutzes von Menschen, die über einen gefährlichen Angriff oder eine kriminelle Verbindung Auskunft erteilen können, auch auf Angehörige dieser Personengruppe
Die rechtlichen Grundlagen für die Tarnung von Unterstützungsmassnahmen bei der Durchführung von Observationen oder verdeckten Ermittlungen wurden ebenfalls geändert. Vor dem Hintergrund extremistischer Entwicklungen wurden am 1. Oktober 2000 Bestimmungen über die erweiterte Gefahrenerforschung mit den entsprechenden Rechtsschutzregelungen in das SPG aufgenommen. [29] Mit diesen Bestimmungen ist den Sicherheitsbehörden nun die Beobachtung von

[22] § 21 Abs. 3 SPG
[23] § 54 SPG
[24] § 42 SPG
[25] § 54 Abs. 2 SPG
[26] § 39 SPG
[27] § 28a SPG

[28] § 38 Bankwesengesetz (BWG)
[29] §§ 21 Abs. 3, 53 Abs. 1 Z. 2a, 54 Abs. 2 und 62a SPG

Gruppierungen möglich, wenn damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommen könnte. Davor waren die Sicherheitsbehörden erst dann zur Beobachtung von extremistischen Gruppierungen ermächtigt, wenn diese bereits kriminell agierten.

Am 1. Dezember 2002 wurde in der Sektion II des Bundesministeriums für Inneres das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung eingerichtet. [30] Es ist dem Generaldirektor für die öffentliche Sicherheit unmittelbarer unterstellt. Dieses übt seine Tätigkeit im Rahmen des Sicherheitspolizeigesetzes (SPG) und, soweit es im Dienste der Strafjustiz tätig wird, nach den Bestimmungen der Strafprozessordnung (StPO) aus.

3. Frankreich

Frankreich ist eine zentralistisch organisierte Demokratie. Die 26 Regionen verfügen im Gegensatz zu den Schweizer Kantonen über keine eigentliche Autonomie.
Der Premierminister ist direkt für die Innere Sicherheit zuständig, wobei er vom Generalsekretariat für nationale Verteidigung (SGDN)[31] und von einem Militärkabinett unterstützt wird. Mit der Inneren Sicherheit sind verschiedene Staatsdienste befasst. Infolgedessen besteht keine eigentliche Trennung von Prävention und Repression.

Frankreich besitzt zwei unabhängige Sicherheitsdienste: Die Polizei und die Gendarmerie Nationale. Die Gendarmerie ist für alle ländlichen Regionen zuständig ist, die Polizei für die Stadtgebiete. Die mobile Gendarmerie ist für die Aufrechterhaltung der öffentlichen Ordnung sowie die Bekämpfung des Terrorismus, des organisierten Verbrechens und der Sekten zuständig. Die nationale Polizei untersteht dem Innenministerium und wird von der Generaldirektion der nationalen Polizei (DGPN)[32] geleitet. Sie vereint zahlreiche Subdirektionen unter ihrem Dach, u. a. die Direktion des Inlandsgeheimdienstes (D.S.T.)[33], die Zentraldirektion des Verfassungsschutzes (RG)[34] und die Koordinationsstelle für Terrorismusbekämpfung. [35]
Die D.S.T. nimmt die Stellung eines Nachrichtendienstes ein und hat den Auftrag, die Verbrechen gegen die Sicherheit des Staates zu bekämpfen.[36] Ihre genaue Organisation und die Funktion sind in einem geheimen Beschluss vom 8. März 1993 geregelt. Die D.S.T. als zentrale Stelle sammelt und bearbeitet sämtlicher Informationen, die ihr von den RG übermittelt werden und sorgt für deren Weitergabe. Zudem beteiligt sich die D.S.T. am Schutz sensibler Bereiche und Geheimnisse der Landesverteidigung. Die RG betreiben ein Informationssystem, zu welchem auch die D.S.T. Zugriff hat. [37]
Die Koordinationsstelle für Terrorismusbekämpfung koordiniert die Arbeit aller Dienste, die im In- und Ausland mobilisiert sind.
Das SGDN ist eine interministerielle Behörde und ist u.a. für die Sicherheit der Informationssysteme, für die Terrorprävention- und Abwehr, für die Absicherung der

[30] § 7 Abs. 1 und 9 Bundesministeriengesetz
[31] Secrétariat Générale de la Défense Nationale
[32] Direction Générale de la Police Nationale
[33] Direction de la surveillance du territoire
[34] Renseignements généraux
[35] Unité de coordination de la lutte antiterroriste
[36] Dekret Nr. 82-1100 vom 22. Dezember 1982, aktualisiert am 15. September 2004
[37] Dekrete Nr. 91-1052 und NR 91-1051

Steuerungs- und Kommunikationsstrukturen der Regierung und Bekämpfung der Proliferation von Atomwaffen verantwortlich und überwacht die Ausfuhr von Kriegsmaterial.
Die Generaldirektion für äussere Sicherheit (DGSE)[38] ist dagegen ist als Auslandsgeheimdienst für die äussere Sicherheit Frankreichs zuständig. Diese untersteht dem Premierminister und ist mit der Informationsbeschaffung und Intervention befasst.
Die Einsichtsrechte in die Informationssysteme der RG erfolgen in der Regel nach dem so genannten indirekten Verfahren.[39] Das Einsichtsgesuch muss bei der unabhängigen „Commission nationale de l'information et des libértés" (CNIL) eingereicht werden. Diese überprüft die Informationen und orientiert den Gesuchsteller, falls Berichtigungen vorgenommen wurden. Wenn die Innere Sicherheit nicht gefährdet ist, können die Daten dem Gesuchsteller mitgeteilt werden. Falls die Datenbank Informationen umfasst, deren Bekanntgabe an die betroffene Person den Zweck der Datenbank nicht gefährdet, kann der Verantwortliche der Datenbank dem Betroffenen direkt informieren.
Es können präventive Telefonüberwachungen im Interesse der inneren Sicherheit angeordnet werden zum volkswirtschaftlichen Schutz Frankreichs, für die Terrorprävention und Bekämpfung der organisierten Kriminalität und bei rechtswidrigen Gruppierungen.[40] Gemäss Art. 4 des Gesetzes vom 10.Juli 1991 wird die Bewilligung durch Beschluss des Premierministers oder zweier durch ihn ernannter Personen erteilt, auf Antrag des Verteidigungsministers, des Innenministers und des Ministers für Zollwesen oder ihrer Stellvertreter. Die Zahl der gleichzeitig vollziehbaren angeordneten Massnahmen sind durch den Premierminister mittels Kontingenten begrenzt und wird durch eine verwaltungsunabhängige „Commission nationale de contrôle des interceptions de sécurité" überwacht. [41] Diese besteht aus einem Präsidenten, welcher für eine Dauer von 6 Jahren durch den Präsidenten der Republik gewählt wird und weiteren Personen. Die Bewilligung wird höchstens für 4 Monate erteilt und kann unter den gleichen Bedingungen jeweils für höchstens weitere 4 Monate verlängert werden. Die gewonnen Erkenntnisse der Überwachung müssen spätestens nach 10 Tagen nach Ausführung unter Aufsicht des Premierministers zerstört werden.
Gemäss Kommission sind alle Informationen im Zusammenhang mit den präventiven Abhörungen als „Secret-Défense" zu klassifizieren. Das heisst u.a., dass Personen die präventiv abgehört wurden, nicht zu informieren sind, weil dies der „défense nationale" grosse Schäden zufügen könnte. Den Staatsschutzbehörden Frankreichs ist hingegen die Postüberwachung untersagt.
Es können des Weiteren in Ausnahmefällen per begründeten Beschluss Einziehungen vorgenommen und Wertgegenstände gesperrt werden, wenn die innere Sicherheit es erfordert[42]. Die Durchführung von Befragungen ist vorgesehen. Des Weiteren sind Durchsuchungen von Fahrzeugen und Hausdurchsuchungen ohne richterliche Prüfung erlaubt. [43] Bei organisierter Kriminalität sind Einätzte auch in der Nacht zugelassen.

[38] Direction Générale de la Sécurité Extérieure
[39] Loi pour la sécurité intérieure" (LOI n° 2003-239 vom 18. März 2003; nachfolgend Gesetz vom 18. März 2003)
[40] Art. 3 Gesetz Nr. 91-646 vom 10. Juli 1991 (Loi relative au secret des correspondances émises par la voie des télécommunications; nachfolgend Gesetz vom 10.Juli 1991)
[41] Art. 5 Gesetz vom 10. Juli 1991
[42] Art. 3 Gesetz vom 18. März 2003 und Gesetz Nr. 2005-750 vom 4. Juli 2005 (Loi n° 2005-750)
[43] Gesetz Nr. 2004-204 vom 9. März 2004 (nachfolgend Gesetz vom 9. März 2004)

Was die verdeckten Bild- und Tonaufzeichnungen, Tarnpapieren und Tarnkennzeichen betrifft**,** wurden verschiedene Kompetenzen mit dem Gesetz vom 18. März 2003 begründet: Demnach sind beispielsweise direkte Zugriffe auf Informationssysteme und das Einholen von Auskünften bei Banken oder Privaten erlaubt**.** Betätigungsverboten können unter bestimmten Umständen ausgesprochen werden, namentlich bei bewaffneten Demonstrationen und bei Organisationen, welche die Sicherheit Frankreichs gefährden würden. [44] Im Rahmen der organisierten Kriminalität ist der Einsatz von Vertrauensleuten vorgesehen, mit nachträglicher Benachrichtigung des Staatsanwaltes. Für deren Abgeltung existieren Spezialfonds. [45]

In Frankreich ist kein parlamentarisches Kontrollsystem vorgesehen, jedoch sind diesbezüglich verschiedene Gesetzesprojekte in Bearbeitung**.** Indessen muss die Regierung dem Parlament Rechenschaftsberichte abliefern.
Die Bekämpfung des Terrorismus hat seit den Anschlägen vom 11.9.2001 auch in Frankreich höchste Priorität. Obwohl die Franzosen namentlich im Kampf gegen den Terrorismus seit Jahrzehnten Erfahrung haben, wurden eine Reihe von neuen Gesetzen und Dekreten erlassen.

4. Italien

Italien ist im Gegensatz zu den Bundesstaaten Schweiz, Deutschland, oder Österreich ein dezentralisierter Einheitsstaat. Die Regionen haben weitgehende Befugnisse in den speziellen Bereichen, u.a. Landwirtschaft, Gesundheits- und Bildungswesen sowie Gemeindepolizeiaufsicht
Die Wahrung der inneren und äusseren Sicherheit ist in Italien auf drei Pfeiler aufgebaut: Den SISMI (Servizio per le informazioni e la sicurezza militare), den SISDE (Servizio per le informazioni e la sicurezza democratica) und die Direzione Investigativa Antimafia (D.I.A.).
Deren Wahrung liegt in der Zuständigkeit des Innenministeriums. Ihm unterstellt ist die „Direzione centrale per la Polizia di Prevenzione“. [46]
Die „Polizia di Prevenzione“ hat folgende Zielsetzungen: die Bekämpfung von internen und externen Terrororganisationen und von paramilitärischen und gewalttätigen Gruppierungen. So können aufgrund von Art. 6 des Gesetzes 121 Daten klassifiziert, analysiert und evaluiert werden, um die Sicherheit zu gewährleisten.
Während der SISMI für die Aktivitäten zuständig ist, die im Ausland stattfinden, ist es der SISDE für die im Inland. Zu den Aufgaben des SISDE gehören die Bekämpfung von Terrorismus, illegaler Einwanderung, Computerkriminalität, Wirtschaftsspionage, neu aufkommender Bedrohungen und organisierter Kriminalität.
Die SISDE sammelt Daten zum Schutz der inneren Sicherheit. Im Allgemeinen besteht ein Einsichtsrecht.[47] Alle Dokumente und Akten, deren Veröffentlichung die Sicherheit des Staates gefährden würde, unterstehen jedoch dem Staatsgeheimnis.[48]
Der Datenschützer (Garante per la protezione dei dati personali) übt die Kontrolle

[44] Gesetz vom 10 Januar 1936 (
[45] Gesetz vom 9. März 2004
[46] Gesetz „legge n. 121 del 1981 Nuovo ordinamento dell’Amministrazione della pubblica sicurezza“; nachfolgend Gesetz 121
[47] „Decreto legislative del 30 giugno 2003, n 196“, nachfolgend Dekret 196
[48] Art. 12 Gesetz vom 24. Oktober 1997

über die gesammelten Daten aus. Die Staatsschutzbehörden arbeiten im Rahmen der Informatiksicherheit mit den Behörden der Kriminalpolizei zusammen.
Die Aktivitäten der SISMI und SISDE werden von einer parlamentarischen Kommission überwacht. Die Regierung muss dem Parlament pro Semester ein Rechenschaftsbericht über die Aktivitäten der Dienste abliefern. Auch sind die Aktivitäten der Nachrichtendienste der Kontrolle der Justiz unterstellt.
Die „Direzione Investigativa Antimafia (D.I.A.) führt Massnahmen gegen die organisierte Kriminalität durch, wie Überwachungen, u.a. auch telefonische Überwachungen und ermittelt gegen die Mafia.[49] Sie kann Informationen beschaffen betreffend finanzielle Verhältnisse der Personen, die verdächtigt werden, kriminellen Organisationen anzugehören. Die D.I.A. gibt die gesammelten Informationen an die SISDE und SISMI weiter. Zudem arbeitet die D.I.A. mit den Polizeikräften zusammen.
Grundsätzlich dürfen Daten nur mit Einverständis der Betroffenen bearbeitet werden, ausser wenn die Datenbearbeitung aufgrund eines gesetzlichen Auftrages erfolgt.[50]
Aufgrund des Gesetzesdekretes vom 27. Juli 2005 sind eine Reihe von zusätzlichen weiteren Kompetenzen und Massnahmen für die Staatschutzbehörden eingeführt worden:[51] Neu sind bei begründetem Terrorverdacht oder bei Gefährdung der Staatsordnung präventive Telefonüberwachungen möglich. Der Antrag ist in der Regel im Voraus durch den Ministerpräsidenten zu begründen. Dieser kann seine Befugnisse an die Nachrichtendienste delegieren. Die Anordnung erfolgt unter Einwilligung des Richters durch die Staatsanwaltschaft. Ist Gefahr in Verzug, kann auch ohne richterliche Einwilligung angeordnet werden. Spätestens nach 24 Stunden muss beim Richter auf dem ordentlichen Weg aber die Bewilligung eingeholt werden. Der Richter muss innerhalb von 48 Stunden über den Antrag entscheiden. Falls diese Frist nicht eingehalten werden kann, so sind die gewonnenen Erkenntnisse nicht gerichtsverwertbar.
Des Weiteren wurde mit dem bis Ende Dezember 2007 befristeten Gesetz 675 die Pflicht zur Aufbewahrung von Telefon - und Internetdaten für die Telekommunikationsgesellschaft und Internetprovider eingeführt. Das Verhör von Gefangenen ohne Anwesenheit eines Verteidigers (colloquio investigativo), welches bislang auf Mafia-Delikte beschränkt war, ist nun auch für die Staatsschutzbehörden gestattet.
Schliesslich wurde die Möglichkeit der erleichterten Ausschaffung von Verdächtigen geschaffen, die eine Gefahr für die öffentliche Sicherheit darstellen oder in irgendeiner Art eine terroristische Organisation unterstützen. Die Ausschaffung wird unverzüglich vollzogen, kann aber vor dem Verwaltungsgericht angefochten werden. Stützt sich der Ausschaffungsentscheid auf geheimdienstliche Quellen, so kann die Gerichtsverhandlung um zwei Jahre aufgeschoben werden. Die Ausschaffungsverfügung kann suspendiert werden, wenn der Auszuschaffende mit den Behörden kooperiert. Im Fall einer für die Ermittlungen massgeblichen Kooperation in Terrorismusermittlungen kann eine Niederlassungsbewilligung gewährt werden.
Bei Missbrauch kann die Bewilligung wieder entzogen werden.

[49] „legge n. 410 del 1991“ ;nachfolgend Gesetz 410
[50] Art. 12 Abs. 1 „legge n. 675 del 31 dicembre 1996 Tutella delle persone e di altri soggetti rispetto al trattamento die dati personali“,nachfolgend Gesetz 675 genannt
[51] Testo del decreto-legge 27 luglio, n.144, coordinato con la legge die conversione 31 luglio 2005 (nachfolgend Gesetz vom 27. Juli 2005)

Mit dem Gesetz vom 27. Juli 2005 wurde für das Innenministerium schliesslich die Möglichkeit zur Einrichtung von polizeicorpsübergreifenden Anti-Terrorismuseinheiten (unità investigative interforze) geschaffen.

5. Luxemburg

Luxemburg ist eine konstitutionelle Monarchie in Form einer parlamentarischen Demokratie und in drei Distrikte mit zwölf Kantonen und 118 Gemeinden gegliedert. Die exekutive Gewalt wird vom Großherzog und der Regierung ausgeübt. Diese setzt sich zusammen aus dem Premierminister, zwölf Ministern, einem delegierten Minister und einer Staatssekretärin.
In Luxemburg sind drei Institutionen mit dem präventiven Staatsschutz befasst: Der für die innere Sicherheit zuständige zivile Nachrichtendienst (SRDE)[52], ferner der zivile Nachrichtendienst, zuständig für die äussere Sicherheit (HCSE)[53] und der militärische Nachrichtendienst.[54] Der SRDE ist dem Innenministerium unterstellt.
Die Kompetenzbereiche des SRDE sind einerseits die Bekämpfung des Terrorismus, der Spionage, der Proliferation von nicht konventionellen Waffen und damit betreffenden Technologien und der organisierten Kriminalität in diesem Geltungsbereich. Andererseits sind es alle Aktivitäten, welche die Integrität, die Souveränität und die Unabhängigkeit des Landes, die Sicherheit der Institutionen und das Funktionieren des Staates oder die Sicherheit des Volkes gefährden können.[55] Im Rahmen ihrer Befugnisse arbeitet der SRDE einerseits mit den polizeilichen-, den gerichtlichen Behörden und mit der Verwaltung und andererseits mit dem HCSE zusammen. Die Polizei und Gerichtsbehörden sowie die Verwaltung sind ihrerseits verpflichtet, Informationen im Geltungsbereich von Art. 2 des Organisationsgesetzes vom 15. Juni 2004 an den SRDE weiterzuleiten.

Die Bearbeitung von Personendaten durch den SRDE richtet sich nach den Bestimmungen des „Loi du 2 août 2002".[56] Der SRDE hat Zugriff zu einer begrenzten Anzahl von Datenbanken, namentlich zur allgemeinen Polizeidatenbank, zur Ausländerdatenbank der Fremdenpolizei und zur Verkehrsdatenbank[57]. Die Aufsichtskontrolle wird durch den Generalstaatsanwalt oder einer seiner Delegierten wahrgenommen und zwei vom Minister gewählten Vertreter einer Spezialkommission. Diese haben Zugang zu den bearbeiteten Daten des SRDE, veranlassen die nötigen Berichtigungen und informieren die betroffenen Personen darüber, dass von ihnen gesetzeskonform Informationen über sie bearbeitet werden.

Bei Belangen der organisierten Kriminalität und der äusseren .Sicherheit[58] kann der Regierungspräsident auf Antrag des SRDE und im Einverständnis mit einer Spezialkommission präventive Telefonüberwachungen anordnen.[59] Die Überwachung muss nach drei Monaten eingestellt werden, kann aber jeweils um

[52] „le Sevice de Renseignement de l'Etat
[53] „La Haute Commissariat de la Sécurité Extérieure
[54] „2ième Bureau de l'Armée".
[55] « Loi du 15 juin portant organisation du Service de Renseignement de l'Etat » (nachfolgend Organisationsgesetz vom 15. Juni 2004)
[56] « Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel » (nachfolgend Gesetz vom 2. August 2002)
[57] Art. 4 des Organisationsgesetzes vom 15. Juni 2004
[58] „Sécurité exterieure de l'Etat"
[59] Art. 88-3 des Code- Pénal und nach dem „Loi du 26 novembre1982[59]"

weitere drei Monate verlängert werden. Erkenntnisse, die im Rahmen einer Telefonüberwachung gewonnen worden sind, sind gerichtlich nicht verwertbar, wenn die betreffende Person ein Berufsgeheimnisträger im Sinne von Art. 458 des Code pénale ist und sie nicht in Verdacht steht, eine strafbare Handlung begangen zu haben oder eine solche zu planen. Der Chef des SRDE muss in diesem Fall die entsprechenden Unterlagen sofort vernichten. Die Beschlüsse der Kommission müssen an den jeweiligen Direktor der Telekommunikationsdienste weitergeleitet werden, welcher sodann die Abhörungen durch eine dafür geschaffene Stelle vollziehen und kontrollieren lässt. Nach Beendigung der Massnahmen erhalten die Betroffenen die kopierten Unterlagen der gewonnenen Erkenntnisse, sofern diese nicht als geheim klassifiziert worden sind. Werden während der fraglichen Zeit keine Resultate erzielt, müssen sämtliche Unterlagen vernichtet werden, ansonsten erst nach Beendigung des Verfahrens.

Die Aktivitäten des SRDE sind der Kontrolle der Kommission unterstellt, welche sich aus Vorsitzenden der im „Chambre des Députés" vertretenen politischen Gruppen zusammensetzt. Der Direktor des Nachrichtendienstes informiert über die allgemeinen Aktivitäten seines Dienstes. Die Kommission kann Einsicht in die Dossiers verlangen und die mit den Dossiers befassten Agenten befragen. Sie verabschiedet einen an den Premierminister, den Chef des Nachrichtendienstes und die Deputierten der Kontrollkommission adressierten vertraulichen Schlussbericht, welcher auch die Observationen, Schlussfolgerungen und Empfehlungen beinhaltet. Die parlamentarische Kontrollkommission wird alle sechs Monate über die durchgeführten Massnahmen betreffend die präventive Telefonüberwachung informiert.

Es können weder Einziehungen und Durchsuchungen durchgeführt werden noch sind Befragungen vorgesehen. Der Premierminister kann unter Einsatz von angemessenen technischen Mitteln die Überwachung jeglicher Form der Kommunikation anordnen, wenn der Verdacht besteht, dass die Sicherheit des Staates gefährdet sei.[60] Die auf diese Weise gesammelten Informationen dürfen den zuständigen Stellen nur beschränkt weitergegeben werden; nämlich nur der Name, Vorname und wenn vorhanden IP-Adresse.[61] Betätigungsverbote können nicht ausgesprochen werden.

6. Niederlande

Die Niederlande ist eine konstitutionelle Monarchie. Die Königin ist Mitglied der Regierung und ernennt die Minister. Das Parlament besteht aus zwei Kammern. Die Zweite Kammer ist das Parlament im eigentlichen Sinne, als Volksvertretung und Kontrolle der Regierung.
Zum niederländischen Nachrichtendienst gehören die folgenden Institutionen: Der zivile Nachrichtendienst (AIVD)[62], der militärische Nachrichtendienst, zu welchem der eigentliche militärische Nachrichtendienst zählt (MIVD)[63], der militärische

[60] Art. 88-3 des „Code de procédure criminelle
[61] Loi du 30 mai 2005 relative à la protection de la personne à l'égard du traitement de données à caractère personnel dans le secteur de communications électroniques
[62] „Algemene Inlichtingen- en Veiligheidsdienst " (General Intelligence and Security Service)
[63] „Inlichtingen- en Veiligheidsdienst" (Military Intelligence and Security Service)

Spezialdienst (BD)[64] und schliesslich der Anti-Terrordienst[65]. Die Zusammenarbeit zwischen dem AIVD und der Polizei ist seit den Anschlägen vom 11.09.01 stark intensiviert worden.
Die Bekämpfung des Terrorismus zählt zu den wichtigsten Zielen des zivilen AIVD. Die AIVD und MIVD führen Ermittlungen sowie Sicherheitsüberprüfungen und Massnahmen gegen Organisationen und Personen durch, die im Verdacht stehen, eine Gefahr für die Sicherheit, die demokratische Ordnung oder andere wesentlichen Staatsinteressen darzustellen.[66] Sie arbeiten mit den Polizei- und Strafverfolgungsbehörden über die Staatsanwaltschaft zusammen, indem Informationen in Form eines Berichts weitergegeben werden. Der AIVD ist befugt, den regionalen Nachrichtendiensten (RID) und dem Spezialsicherheitsdienst der königlichen Militärpolizei zu beantragen, in seinem Auftrag tätig zu werden.
Grundsätzlich haben Betroffene auf Verlangen umfassendes Einsichtsrecht in die Daten, die in Zusammenhang mit den gegen sie getroffenen Massnahmen erhoben worden sind; der Quellenschutz bleibt jedoch gewahrt. Die Einsichtsrechte werden eingeschränkt, sofern die Offenlegung der Daten eine Gefährdung der inneren Sicherheit zur Folge hätte. Über das Nichteintreten muss die dafür zuständige Aufsichtskommission informiert werden. [67] Diese wacht über die Tätigkeit der Dienste und unterrichtet die zuständigen Minister.
Der AIVD und der MIVD sind ermächtigt, präventive Post- und Fernmeldeüberwachungen durchzuführen. Der Antrag erfolgt zum Voraus unter Bewilligung des Verteidigungsministers durch den Chef des AIVD und des MIVD und im Einverständnis des Innenministers. Ist Gefahr in Verzug, ist eine nachträgliche Genehmigung unter der Voraussetzung zulässig, dass diese so schnell wie möglich eingeholt wird.
Des Weiteren sind die Dienste bei schriftlicher Einwilligung des zuständigen Ministers ermächtigt, Observationen unter Einsatz von technischen Mitteln auszurichten. Die Observation und Durchsuchungen privater Räume sind in Absprache mit dem Innenminister oder dem Chef der Dienste erlaubt. Auch sind Einsätze unter einer Tarnidentität vorgesehen und erlaubt Briefe Dritter zu öffnen, sofern das Bezirksgericht Den Haag einem Antrag des Chefs der Dienste entspricht. Das Eindringen in fremde EDV-Systeme ist ebenfalls gestattet, sofern der Innenminister oder der Chef der Dienste ihr Einverständnis abgeben. Dagegen hat es keine ausdrücklichen Regelungen für die Beschlagnahme, Einziehung und Sicherstellung von Gegenständen noch für Betätigungsverbote gegen Einzelpersonen oder Organisationen:
Der von der Regierung unabhängiger „Nationaler Ombudsmann“ wacht u.a. über die Tätigkeiten der Dienste. Sein Einflussbereich gegenüber den Diensten wurde aber mit einer Revision weiter eingeschränkt.[68] Die Dokumente der Dienste sind zwar einsehbar, können aber nicht kopiert werden.
Der zuständige Minister informiert die parlamentarische Aufsichtskommission regelmässig über die Tätigkeiten der Dienste.

[64] „Koninklijke Marechaussee, Bijzondere Dienst en Veiligheid“ (Military policeSpecial section for intelligence and security)
[65] („Bijzondere Bijstands Eenheid“ (Special Help Union Anti-Terrorist Service).
[66] „Act of 7 February 2002, providing for rule s relating to the intelligence and security services and amendment of several acts (Intelligence and Security Services Act 2002)”
[67] Supervisory committee
[68] „Act of 3 February 2005“

7. EU

Die Eu verfolgt seit den Anschlägen vom 11. September 2001 in den USA eine gezielte Politik zur Terrorismusbekämpfung. Im Nachgang zu den Bombenanschlägen in London sprach sich die EU anlässlich eines Sondertreffens der europäischen Innen- und Justizminister in Brüssel für eine engere Zusammenarbeit der 25 EU- Staaten im Anti-Terror- Kampf aus. Es wurde eine bessere Zusammenarbeit von Polizei und Geheimdiensten über die Grenzen hinweg gefordert.
Am 21. September 2005 hat die EU-Kommission ein umfassendes Paket von 4 Massnahmen vorgestellt.
- Vorschlag für eine Richtlinie über die Aufbewahrung von Verkehrsdaten durch Dienstanbieter:
Der Vorschlag stellt auf die Harmonisierung der Pflichten für Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten bzw. Betreiber eines öffentlichen Kommunikationsnetzes im Zusammenhang mit Vorratsspeicherfristen von einem Jahr für Verkehrsdaten von Gesprächen im Fest- und Mobilfunknetz, bzw. von sechs Monaten für Verkehrsdaten, die sich auf die Nutzung des Internets beziehen, ab.
-Finanzbeschluss über 7 Mio. Euro für ein Pilotprojekt auf dem Gebiet der Prävention, Abwehrbereitschaft und Reaktion im Zusammenhang mit Terroranschlägen:
Der Finanzbeschluss stellt darauf ab, die Strafverfolgungsbeteiligten zu vernetzen, um Informationsaustausch und Krisenmanagement zu vereinfachen. Zudem dient er zur Unterstützung des geplanten Europäischen Programms zum Schutz kritischer Infrastrukturen.
- Vorschlag für einen Beschluss des Rates über die Unterzeichnung der Konvention 198 des Europarates über Geldwäsche, Terrorismusfinanzierung sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten:
Der Vorschlag regt die 46 Mitgliederländer an, dass sie die gleichen strengen Vorschriften gegen die Geldwäsche einführen, wie sie bereits in der EU gelten und eine einheitliche Front im Kampf gegen die Terrorismusfinanzierung bilden.
-Mitteilung „Rekrutierung von Terroristen: Bekämpfung der Ursachen von Radikalisierung und Gewaltbereitschaft:
Die Mitteilung ist der im Haager Programm vorgesehene Beitrag der Kommission für diesen Bereich. Der Rat muss bis Ende Jahr eine Strategie ausarbeiten. In ihr werden mögliche Lösungen für ein effizientes Herangehen an diese Frage in unterschiedlichen Bereichen wie Internet, Zusammenarbeit zwischen den Strafverfolgungsbehörden und Geheimdiensten der Mitgliedstaaten und Aussenbeziehungen vorgeschlagen.