14.xxx

Botschaft zum Nachrichtendienstgesetz

vom 19. Februar 2014

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf des Nachrichtendienstgesetzes.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

19. Februar 2014

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Didier Burkhalter
Die Bundeskanzlerin: Corina Casanova

Übersicht

Diese Vorlage soll eine einheitliche, formellgesetzliche Grundlage für den zivilen Nachrichtendienst der Schweiz, den Nachrichtendienst des Bundes (NDB), schaffen. Der NDB beschafft Informationen, analysiert diese, wertet sie aus und leitet sie weiter mit dem Ziel, Entscheidungsträger aller Stufen mit Informationen zu versorgen, die diese benötigen, um ihre Führungsaufgabe situations- und zeitgerecht wahrnehmen zu können.

Der NDB gehört gemäss dem aktuellen sicherheitspolitischen Bericht – wie die Aussenpolitik, die Armee und die Polizei – zu den sicherheitspolitischen Instrumenten des Bundes.

Das zentrale Anliegen der Vorlage besteht darin, Tätigkeit, Beauftragung und Kontrolle des Nachrichtendienstes gesetzlich zu regeln. Damit soll der NDB in die Lage versetzt werden, im Sinne der Prävention einen substanziellen Beitrag zur Sicherheit der Schweiz und ihrer Bevölkerung zu leisten.

Ausgangslage

Praktisch zeitgleich mit der Verabschiedung des Bundesgesetzes vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) beschloss der Bundesrat in einem ersten Schritt die Überführung der nachrichtendienstlichen Teile des Dienstes für Analyse und Prävention (DAP) ins Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) auf den 1. Januar 2009. In einem zweiten Schritt führte er auf den 1. Januar 2010 den Strategischen Nachrichtendienst (SND) und den DAP zum NDB zusammen. Als dritten Schritt beauftragte der Bundesrat schliesslich das VBS mit der Ausarbeitung einer Botschaft zu einem neuen, gesamtheitlichen Nachrichtendienstgesetz bis Ende 2013 (BRB vom 27. November 2009).

Das neue Gesetz soll nach dem Willen des Bundesrates die gesetzliche Grundlage für die Aufgaben, die Rechte und Pflichten und die Informationssysteme des zivilen Nachrichtendienstes schaffen. Der Gesetzesentwurf soll keine Weiterentwicklung der bestehenden Rechtsgrundlagen darstellen, sondern eine Neukodifikation, die bestehenden Bedenken und Vorbehalten gegenüber der bisherigen Tätigkeit der Nachrichtendienste in der Schweiz (insbesondere betreffend das Sammeln von Personendaten) weitestmöglich Rechnung trägt und die veränderten Risiken und Bedrohungen besser berücksichtigt.

Inhalt der Vorlage

Der vorliegende Gesetzesentwurf enthält im Wesentlichen folgende Neuerungen:

- Gesamtheitliche Gesetzesgrundlage für den NDB: *Die bisherige Zweiteilung in das ZNDG und das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) entfällt.*
- Neuausrichtung der Informationsbeschaffung: *Es wird nicht mehr primär zwischen Bedrohungen aus dem Inland und aus dem Ausland unterschieden,*

sondern zwischen gewalttätigem Extremismus mit Bezug zur Schweiz einerseits und den übrigen Bedrohungsfeldern und Aufgaben andererseits.

- Einführung von neuen Informationsbeschaffungsmassnahmen in den Bereichen Terrorismus, verbotener Nachrichtendienst, Proliferation und Angriffe auf kritische Infrastrukturen oder zur Wahrung weiterer wesentlicher Landesinteressen: *Die in der Vorlage BWIS II vom Parlament zurückgewiesenen besonderen Beschaffungsmittel wie die Überwachung des Post- und Fernmeldeverkehrs oder der Einsatz von technischen Überwachungsgeräten im privaten Bereich werden in überarbeiteter Form vorgeschlagen und ergänzt. Die neuen Beschaffungsmassnahmen sind nach Auffassung des Bundesrates notwendig. Das heutige Instrumentarium reicht nicht mehr aus, um die präventiven Aufgaben des NDB angesichts der immer aggressiveren Akteure, die die innere oder die äussere Sicherheit der Schweiz bedrohen und angesichts der komplexeren Bedrohungsformen weiterhin wahrzunehmen. Eine gerichtliche und eine politische Instanz sollen im Einzelfall über die Genehmigung der neuen Massnahmen entscheiden.*
- Differenzierte Datenerfassung und -haltung: *Der Entwurf sieht vor, dass die vom NDB beschafften oder bei ihm eintreffenden Meldungen je nach Thematik, Quelle und Sensibilität der Daten in einem Verbund von Informationssystemen abgelegt werden. Bevor Personendaten des NDB eine Aussenwirkung entfalten, indem sie in einem Produkt des NDB (z.B. Analysebericht, Meldung an ausländischen Nachrichtendienst, Lagebeurteilung) verwendet werden, müssen sie auf Richtigkeit und Erheblichkeit geprüft werden. Daten, die der NDB mittels einer genehmigungspflichtigen Beschaffungsmassnahme erhält, werden gesondert behandelt und stehen nur den Spezialistinnen und Spezialisten innerhalb des NDB zur Verfügung.*
- Kontrollregime: *Die Tätigkeiten des NDB unterliegen einer dreifachen Kontrolle bzw. Aufsicht, nämlich durch das vorgesetzte Departement, durch den Bundesrat und durch die Geschäftsprüfungsdelegation des Parlaments. Die Funkaufklärung unterliegt zusätzlich einer gesonderten fachlichen Überprüfung durch die unabhängige Kontrollinstanz. Die genehmigungspflichtigen Beschaffungsmassnahmen sowie die Kabelaufklärung gelangen nur zur Anwendung, wenn das Bundesverwaltungsgericht der betreffenden Massnahme zugestimmt und anschliessend die Chefin oder der Chef des VBS nach Konsultation des Sicherheitsausschusses des Bundesrates die Freigabe für die Durchführung des Einsatzes erteilt hat. Mit diesen Mechanismen soll die Recht- und Verhältnismässigkeit der Tätigkeiten des NDB sichergestellt werden.*

Inhaltsverzeichnis

Übersicht **2**

1 Grundzüge der Vorlage **5**

1.1 Ausgangslage 5

1.2 Die beantragte Neuregelung 8

1.3 Begründung und Bewertung der vorgeschlagenen Lösung 10

1.4 Abstimmung von Aufgaben und Finanzen 16

1.5 Rechtsvergleich, insbesondere mit dem europäischen Umfeld 16

1.6 Umsetzung 35

2 Erläuterungen zu einzelnen Artikeln **35**

3 Auswirkungen **120**

3.1 Auswirkungen auf den Bund 120

3.1.1 Finanzielle Auswirkungen 120

3.1.2 Personelle Auswirkungen 121

3.1.3 Andere Auswirkungen 122

3.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete 122

3.3 Auswirkungen auf die Volkswirtschaft und auf die Gesellschaft 123

3.4 Andere Auswirkungen 123

4 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates **123**

4.1 Verhältnis zur Legislaturplanung 123

4.2 Verhältnis zu nationalen Strategien des Bundesrates 123

5 Rechtliche Aspekte **124**

5.1 Verfassungs- und Gesetzmässigkeit 124

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz 127

5.3 Erlassform 128

5.4 Unterstellung unter die Ausgabenbremse 128

5.5 Einhaltung der Grundsätze der Subventionsgesetzgebung 128

5.6 Delegation von Rechtsetzungsbefugnissen 129

5.7 Datenschutz 130

Nachrichtendienstgesetz *(Entwurf)* **133**

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

Diese Vorlage soll eine einheitliche, formellgesetzliche Grundlage für den Nachrichtendienst des Bundes (NDB) schaffen. Der Nachrichtendienst beschafft Informationen, analysiert diese, wertet sie aus und leitet sie weiter mit dem Ziel, Entscheidungsträgerinnen und -träger aller Stufen mit Informationen zu versorgen, die diese benötigen, um ihre Führungsaufgabe situations- und zeitgerecht wahrnehmen zu können.

Der NDB gehört gemäss dem aktuellen Bericht des Bundesrates an die Bundesversammlung vom 23. Juni 2010[1] über die Sicherheitspolitik der Schweiz (nachfolgend: sicherheitspolitischer Bericht des Bundesrats) wie die Aussenpolitik, die Armee, der Bevölkerungsschutz, die Wirtschaftspolitik, die Zollverwaltung, die Polizei und der Zivildienst zu den sicherheitspolitischen Instrumenten der Schweiz. Er ist Teil der Sicherheitsarchitektur der Schweiz.

Der sicherheitspolitische Bericht des Bundesrates definiert die Rolle des NDB wie folgt:

«Der NDB ist das Kompetenzzentrum für sämtliche nachrichtendienstlichen Belange der inneren und äusseren Sicherheit. Er unterstützt die politische und militärische Führung und weitere Dienststellen bei Bund und Kantonen und trägt mit seinen Erkenntnissen und Beurteilungen zu bedrohungsgerechten und breit abgestützten Entscheiden bei. Der NDB richtet den Einsatz seiner Mittel nach den Bedürfnissen und Erwartungen seiner Partner und Leistungsbezüger aus. So generiert er einen nachrichtendienstlichen Nutzen, mit dessen Hilfe eine umfassende führungsrelevante Nachrichtenlage für Entscheidträger jeglicher Ebenen geschaffen werden soll.»

Der Bundesrat hat mit dieser Definition gleichzeitig den Rahmen abgesteckt, den die Verfassung für die Aufgaben des NDB vorsieht.

Das zentrale Anliegen dieser Vorlage besteht darin, die Tätigkeit, die Beauftragung und die Kontrolle des Nachrichtendienstes gesetzlich zu regeln. Damit soll der NDB in die Lage versetzt werden, im Sinne der Prävention einen substanziellen Beitrag für die Sicherheit der Schweiz und ihrer Bevölkerung zu leisten.

Vorgeschichte und Auftrag des Bundesrates

Im Bericht vom 29. Februar 2008[2] zur Parlamentarischen Initiative: «Übertragung der Aufgaben der zivilen Nachrichtendienste an ein Departement» äusserte sich die Geschäftsprüfungskommission des Ständerates zur Tätigkeit der Nachrichtendienste wie folgt:

«Die Tätigkeit der beiden Dienste [Anm.: Gemeint sind der Dienst für Analyse und Prävention (DAP) und der Strategische Nachrichtendienst (SND)] überschneidet sich in einzelnen Bereichen sowohl der Natur der Sache nach als auch von der gesetzlichen Aufgabenumschreibung her. Einerseits lassen sich die äussere und die

1 BBl **2010** 5133
2 BBl **2008** 4015

innere Sicherheit nicht immer scharf voneinander abgrenzen. Andererseits setzt die Tätigkeit des SND bis zu einem gewissen Grade Aktivitäten im Inland voraus, während der gesetzliche Aufgabenkatalog des DAP auch Auslandkontakte voraussetzt. Eine Kooperation der beiden Dienste ist daher für eine effiziente und erfolgreiche Tätigkeit unabdingbar. …

Im Juni 2005 beschloss der Bundesrat, den Nachrichtenkoordinator abzuschaffen und setzte im Gegenzug auf eine verbesserte Zusammenarbeit zwischen den zivilen Nachrichtendiensten im EJPD [Eidgenössiches Justiz- und Polizeidepartement]und VBS [Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport]. Insbesondere sollten der DAP und der SND grenzüberschreitende Bedrohungen gemeinsam bearbeiten. Zu diesem Zweck beschloss der Bundesrat den Aufbau sogenannter Plattformen für den Informationsaustausch und die gemeinsame Auswertung in den Bereichen Terrorismus, Organisierte Kriminalität und Proliferation.

Im Rahmen ihrer Aufsichtstätigkeit über die Nachrichtendienste und den Staatsschutz hatte die Geschäftsprüfungsdelegation (GPDel) die zuständigen Departemente und den Bundesrat seit längerer Zeit auf die mangelhafte Zusammenarbeit des SND und des DAP hingewiesen. Die Delegation begrüsste deshalb die im Jahr 2005 vom Bundesrat beschlossene Zusammenarbeit in den neuen Plattformen als einen pragmatischen, ersten Reformschritt. Gleichzeitig hielt die GPDel fest, dass diese Massnahmen die politische Führung der Nachrichtendienste nicht verbesserten. Sie wiederholte deshalb ihre Forderung aus dem Jahr 2004, dass die Nachrichtendienste einem einzigen Departement zugeordnet und möglichst rasch einer gemeinsamen Leitung unterstellt werden sollten. Die GPDel erklärte sich aber bereit, vorerst die Reformen des Bundesrats zu begleiten und bis Ende 2006 ihre Wirkung abzuwarten.

… Die Mängel, die sie in ihren Jahresberichten der Jahre 2004, 2005 und 2006 kritisiert hatte, waren nicht behoben worden. Insbesondere musste die GPDel aufgrund zahlreicher Anhörungen und dreier unangemeldeter Besuche bei den Plattformen feststellen, dass die getroffenen Massnahmen die Zusammenarbeit zwischen DAP und SND nur ungenügend verbessert hatten.

… Die GPDel sah deshalb einen dringenden Handlungsbedarf. Die Zusammenarbeit von In- und Auslandnachrichtendienst sollte nicht mehr dem Gutdünken zweier Departemente überlassen bleiben. Vielmehr sollte ein einziges Departement für die Tätigkeit der beiden Nachrichtendienste zuständig sein. Die GPDel beschloss daher einstimmig, mit einer parlamentarischen Initiative die Aufgaben der beiden zivilen Nachrichtendienste einem einzigen Departement zu übertragen.»

Das aufgrund der parlamentarischen Initiative entstandene Bundesgesetz vom 3. Oktober 2008[3] über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) trat am 1. Januar 2010 in Kraft.

Nach der Verabschiedung des ZNDG beschloss der Bundesrat in einem ersten Schritt die Überführung der nachrichtendienstlichen Teile des DAP ins VBS auf den 1. Januar 2009. In einem zweiten Schritt beschloss er im März 2009 die Zusammenführung des SND und des DAP zum NDB auf den 1. Januar 2010.

3 SR **121**

In einem dritten Schritt beauftragte er schliesslich das VBS, bis Ende 2013 eine Botschaft zu einem gesamtheitlichen Nachrichtendienstgesetz vorzulegen (BRB vom 27. November 2009):

«Das VBS wird beauftragt dem Bundesrat

… bis spätestens Ende 2013 eine Botschaft mit einem Entwurf eines neuen Nachrichtendienstgesetzes vorzulegen, in dem eine gesetzliche Grundlage über die Aufgaben, Rechte, Pflichten und Informationssysteme der zivilen Nachrichtendienste für die Schweiz geschaffen wird. Die bestrittenen Punkte der ursprünglichen Botschaft vom 15. Juni 2007 zur Änderung des BWIS[4] *sowie die geltenden Bestimmungen sollen in der Gesetzesvorlage neu geregelt werden.»*

Staffelung der Gesetzgebungsarbeiten gemäss BRB vom 27. November 2009

National- und Ständerat wiesen im Frühjahr 2009 die Vorlage BWIS II vom 15. Juni 2007[5] (Besondere Mittel der Informationsbeschaffung) zur Prüfung von einigen verfassungsrechtlichen Fragen im Zusammenhang mit im Entwurf vorgesehenen nachrichtendienstlichen Beschaffungsmassnahmen, die strafprozessualen Zwangsmassnahmen nachgebildet waren, an den Bundesrat zurück. Zu einer inhaltlichen Auseinandersetzung mit den einzelnen Gesetzesartikeln war es dabei nur im Ständerat gekommen; die parlamentarische Debatte im Nationalrat beschränkte sich auf die Eintretensfrage. Genaue Aussagen über die damalige politische Akzeptanz einzelner Elemente der Vorlage lassen sich deshalb nur beschränkt ableiten.

Der Bundesrat liess in der Folge die verfassungsrechtlichen Fragen durch ein Gutachten prüfen und beschloss eine Staffelung der Gesetzgebungsarbeiten (Bundesratsbeschluss vom 27. November 2009): In einer rasch zu behandelnden ersten Vorlage sollten die mehrheitlich unbestrittenen und entscheidungsreifen Anliegen im BWIS umgesetzt werden. Dieser Teil wurde inzwischen durch die Zusatzbotschaft vom 27. Oktober 2010[6] zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit («BWIS II reduziert») realisiert und vom Parlament am 23. Dezember 2011 verabschiedet. Das revidierte BWIS trat am 16. Juli 2012 in Kraft.

Die zweite Vorlage sollte das hier behandelte Nachrichtendienstgesetz zum Gegenstand haben, das den Nachrichtendienst gesamthaft regelt.

Entstehung des vorliegenden Gesetzesentwurfs

Zur Vorbereitung des neuen Gesetzes setzte der NDB eine interdepartementale Arbeitsgruppe (IDAG) ein. Diese setzte sich zusammen aus Vertreterinnen und Vertretern des VBS, des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA), des EJPD der Bundesanwaltschaft, der Kantone und des NDB. Ein Mitarbeiter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) stand für die Prüfung datenschutzrechtlicher Fragen zur Verfügung.

Die IDAG nahm ihre Arbeiten Ende Oktober 2010 auf und erarbeitete bis im Juli 2011 ein Strategiepapier und ein Normkonzept. Gestützt auf die Vorarbeiten der

4 Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), SR **120**

5 Botschaft vom 15. Juni 2007 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; BBl **2007** 5037)

6 BBl **2010** 7841

IDAG nahm der NDB in der Folge die Redaktion des vorliegenden Gesetzesentwurfs an die Hand. Die Gesetzesentwürfe wurden der IDAG jeweils zur Stellungnahme unterbreitet.

Bewährte Regelungen aus dem BWIS und aus dem ZNDG sowie Neuregelungen aus der Vorlage «BWIS II reduziert» wurden in den Gesetzesentwurf übernommen, soweit dies sinnvoll erschien. So entsprechen beispielsweise die besonderen Auskunfts- und Meldepflichten und das Tätigkeitsverbot dem Grundsatz nach den entsprechenden Bestimmungen aus der Botschaft «BWIS II reduziert».

Das neue Nachrichtendienstgesetz soll aber keine Weiterentwicklung der bestehenden Rechtsgrundlagen (also kein «BWIS III» oder «ZNDG II») sein, sondern eine Neukodifikation, die bestehenden Bedenken und Vorbehalten gegenüber der bisherigen Tätigkeit der Nachrichtendienste in der Schweiz weitestmöglich Rechnung trägt und die veränderten Risiken und Bedrohungen besser berücksichtigt.

Sowohl im Vernehmlassungsverfahren zum Entwurf von 2007 als auch in der bisherigen politischen Auseinandersetzung und in der Berichterstattung der Medien war die Einführung von besonderen Mitteln der Informationsbeschaffung die mit Abstand am kontroversesten diskutierte Massnahme.

Deshalb verzichtete der Bundesrat in seiner Vorlage «BWIS II reduziert» im Wesentlichen auf folgende genehmigungspflichtige Mittel der Informationsbeschaffung:

- Überwachung des Post- und Fernmeldeverkehrs;
- Beobachten an nicht allgemein zugänglichen Orten, auch mittels technischem Überwachungsgerät;
- geheimes Durchsuchen eines Datenverarbeitungssystems.

Diese Punkte wurden dem Grundsatz nach im vorliegenden Entwurf wieder aufgenommen.

Am 8. März 2013 verabschiedete der Bundesrat den Vorentwurf zum Nachrichtendienstgesetz (NDG) und ermächtigte das VBS zur Durchführung eines Vernehmlassungsverfahrens. Dieses dauerte vom 8. März bis zum 30. Juni 2013. Am 23. Oktober 2013 nahm der Bundesrat vom Vernehmlassungsergebnis Kenntnis und beauftragte das VBS mit der Weiterführung der Gesetzgebungsarbeiten.

1.2 Die beantragte Neuregelung

Kernpunkte des Gesetzesentwurfs:

Gesamtheitliche Gesetzesgrundlage für den NDB

Neuausrichtung der Informationsbeschaffung

Der Gesetzesentwurf (E-NDG) sieht bei der Beschaffung von Informationen insofern eine Neuerung vor, als nicht mehr primär zwischen Bedrohungen aus dem Inland und aus dem Ausland, sondern zwischen gewalttätigem Extremismus mit Bezug zur Schweiz und den übrigen Bedrohungsfeldern und Aufgaben unterschieden wird. Eine Konsequenz dieses Konzeptes ist, dass beim gewalttätigen Extremismus genehmigungspflichtige Beschaffungsmassnahmen nicht zur Anwendung gelangen können. Damit soll von den damaligen, von der parlamentarischen Unter-

suchungskommission (PUK) aufgearbeiteten Vorkommnissen im EJPD (Bericht der Parlamentarischen Untersuchungskommission vom 22. November 1989[7] über die Vorkommnisse im Eidgenössischen Justiz- und Polizeidepartement) endgültig Abschied genommen werden, indem eine Trennlinie zwischen Terrorismus und gewalttätigem Extremismus gezogen wird. Wie bei der Datenhaltung soll auch die Beschaffung im Bereich des gewalttätigen Extremismus, der vorwiegend Bezüge zur Schweiz bzw. zu Schweizer Akteuren aufweist, strengeren Auflagen bezüglich Grundrechtseingriffen unterliegen. Der Bundesrat legt nach Artikel 69 Absatz 1 Buchstabe c E-NDG auf einer Liste jährlich fest, welche Gruppierungen als gewalttätig-extremistisch einzustufen sind.

Einführung von neuen Beschaffungsmassnahmen in den Bereichen Terrorismus, verbotener Nachrichtendienst, Proliferation und Angriffe auf kritische Infrastrukturen oder zur Wahrung wesentlicher Landesinteressen nach Artikel 3

Die in BWIS II enthaltenen und vom Parlament zur Überprüfung zurückgewiesenen besonderen Mittel der Informationsbeschaffung wurden hinsichtlich ihrer Verfassungs- und Völkerrechtskonformität begutachtet (Gutachten Prof. Giovanni Biaggini vom Juni 2009[8]). Im vorliegenden Entwurf wurde der in BWIS II enthaltene Katalog der besonderen Informationsbeschaffungsmittel überarbeitet und gleichzeitig ergänzt. Der Bundesrat beantragt die Einführung folgender neuer, genehmigungspflichtiger Informationsbeschaffungsmassnahmen im Inland:

- Überwachung des Post- und Fernmeldeverkehrs gemäss den Bestimmungen des Bundesgesetzes vom 6. Oktober 2000[9] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), inklusive Auskünfte über die Post- und Fernmeldeverbindungen überwachter Personen und Auskünfte über den Standort von Antennen, mit denen das Mobiltelefon einer überwachten Person verbunden ist;
- Einsatz von technischen Ortungsgeräten, um den Standort und die Bewegungen von Personen oder Sachen festzustellen;
- Einsatz von technischen Überwachungsgeräten zur Abhörung oder Aufzeichnung von Privatgesprächen und zum Beobachten oder Aufzeichnen von Vorgängen an nicht öffentlichen Orten;
- Eindringen in Computersysteme und -netzwerke zur Beschaffung von Informationen oder um in bestimmten, wenigen Ausnahmefällen den Zugriff auf Informationen zu stören, zu verhindern oder zu verlangsamen;
- Durchsuchen von Räumlichkeiten, Fahrzeugen oder von Personen mitgeführten Behältnissen.

Voraussetzung für den Einsatz dieser Massnahmen sind die vorgängige Genehmigung durch das Bundesverwaltungsgericht und die anschliessende Freigabe durch die Chefin oder den Chef des VBS, nachdem zuvor der Sicherheitsausschuss des Bundesrates konsultiert wurde.

7 BBl **1990** 637
8 Das Gutachten ist im Internet unter folgender Adresse abrufbar: www.bk.admin.ch > Dokumentation > Verwaltungspraxis der Bundesbehörden VPB > VPB 2009 > 2009.14 (S. 238–330)
9 SR **780.1**

Diese neuen Beschaffungsmassnahmen werden vorgeschlagen, weil das heutige Instrumentarium (Art. 14 BWIS) angesichts der immer aggressiveren und komplexeren Bedrohungsformen nicht mehr ausreicht, um die präventive Aufgabe des Nachrichtendienstes im Bereich der inneren Sicherheit wahrzunehmen. Im Übrigen wird auf die Erläuterungen zu Artikel 25 ff. (genehmigungspflichtige Beschaffungsmassnahmen) verwiesen.

Nachvollzug der technischen Entwicklung bei den genehmigungsfreien Beschaffungsmassnahmen

Die genehmigungsfreien Beschaffungsmassnahmen (Art. 13 ff.) werden ebenfalls erweitert. Vorhandene technische Möglichkeiten (z.B. der Einsatz von Luftaufklärungsmitteln) sollen nutzbar gemacht werden. Für den Einsatz solcher Mittel bestand bisher keine formellgesetzliche Grundlage, weshalb die Rechtslage unklar war.

Differenzierte Datenbearbeitung

Der Entwurf sieht vor, dass die vom NDB beschafften oder bei ihm eintreffenden Meldungen je nach Thematik, Quelle und Sensibilität der Daten in einem Verbund von Informationssystemen abgelegt werden. Bevor Personendaten des NDB eine Aussenwirkung entfalten, indem sie in einem Produkt des NDB (z.B. Analysebericht, Meldung an ausländischen Nachrichtendienst, Lagebeurteilung) verwendet werden, müssen sie auf Richtigkeit und Erheblichkeit bewertet werden. Daten, die der NDB mittels einer genehmigungspflichtigen Beschaffungsmassnahme oder aufgrund von Grenzkontrollen erhält, werden gesondert behandelt und stehen nur den Spezialistinnen und Spezialisten innerhalb des NDB zur Verfügung.

Kontrollregime

Die Tätigkeiten des NDB unterliegen einer dreifachen Kontrolle bzw. Aufsicht, nämlich durch das vorgesetzte Departement, durch den Bundesrat und durch die Geschäftsprüfungsdelegation des Parlaments. Die Funkaufklärung unterliegt weiterhin zusätzlich einer gesonderten fachlichen Überprüfung durch die unabhängige Kontrollinstanz.

Beschwerdemöglichkeiten

Das NDG sieht bei Verfügungen und genehmigungspflichtigen Beschaffungsmassnahmen des NDB Beschwerdemöglichkeiten beim Bundesverwaltungsgericht und in zweiter Instanz beim Bundesgericht vor.

1.3 Begründung und Bewertung der vorgeschlagenen Lösung

Substanzieller Beitrag zur Sicherheit der Schweiz

Die Schweiz ist auf einen leistungsfähigen Nachrichtendienst angewiesen, um ihre Interessen und den Schutz ihrer Bürgerinnen und Bürger zu wahren. Gleichzeitig gilt es, den Freiheitsrechten der Bevölkerung Rechnung zu tragen.

Der NDB und die Vollzugsbehörden der Kantone, haben die Aufgabe, einen substanziellen Beitrag zur Wahrung der Schweizer Interessen und der inneren wie äusseren Sicherheit der Schweiz zu liefern, und zwar unter Wahrung der Freiheits-

rechte der Bürgerinnen und Bürger. Sie sollen die nötigen Informationen mit nachrichtendienstlichen Mitteln und Methoden (das heisst unter Verwendung öffentlicher und nicht öffentlicher Informationsquellen sowie menschlicher Quellen) beschaffen, bearbeiten, auswerten und in geeigneter Form insbesondere an die staatlichen Entscheidungsträger (Bund und Kantone) weiterleiten. Zu diesem Zweck ist eine umfassende Beurteilung der Bedrohungslage unumgänglich. Mit den heutigen gesetzlichen Informationsbeschaffungsmitteln, die das BWIS für den Bereich der inneren Sicherheit vorsieht und die im Wesentlichen auf der Beschaffung aus öffentlichen Quellen, dem Einholen von Auskünften und dem Beobachten an öffentlichen Orten bestehen (Art. 14 BWIS), kann der NDB seine Aufgabe nur bedingt erfüllen. Der Gesetzesentwurf ergänzt deshalb die bisherigen Beschaffungsmassnahmen im Bereich der inneren Sicherheit durch die Einführung von genehmigungspflichtigen Beschaffungsmassnahmen. Er regelt auch die Nachrichtenbeschaffung der Kantone bzw. der kantonalen Vollzugsbehörden.

Der NDB als Ganzes versieht und unterstützt seine Kunden gezielt und zeitgerecht mit Informationen und Beurteilungen, die auf andere Weise nicht erhältlich sind.

Blick auf das internationale Umfeld

Das Nachrichtendienstwesen ist auch im 21. Jahrhundert weitestgehend Sache der Nationalstaaten und damit ein Instrument der jeweiligen politischen Führung eines Landes. Dies gilt für die Schweiz in besonderem Mass. Sie ist als unabhängiger und neutraler Staat in verschiedener Hinsicht auf sich allein gestellt. Unsere Partner in Europa gehören mehrheitlich der North Atlantic Treaty Organization (NATO) und/oder der Europäischen Union (EU) an. Aber auch Gremien wie die G-20 fällen weitreichende Entscheidungen, die die Schweiz ebenfalls betreffen, zu denen unser Land aber kaum konsultiert wird. Gerade die Mitglieder von EU und NATO sind auch im Bereich des Informationsaustauschs eng miteinander vernetzt. Die Mitgliedschaft zahlt sich in einem breiten, permanent unterhaltenen Lagebild aus. Der NDB unterstützt durch seine Kontakte zu den Nachrichtendiensten von ausländischen Staaten und durch die so erhaltenen Informationen die Aussenpolitik der Schweiz.

Erkenntnisse zum «Fall Snowden»

Die jüngst durch den ehemaligen US-Geheimdienstmitarbeiter Edward Snowden ermöglichten Enthüllungen der Medien haben einen neuen Einblick in die Praktiken der grossen internationalen Nachrichtendienste vor allem im Bereich der Kommunikationsüberwachung gegeben. Internationale Nachrichtendienste machen auch vor grundsätzlich befreundeten Staaten nicht halt, wenn die technischen Möglichkeiten für das Eindringen in Kommunikationssysteme gegeben sind. Neu ist auch das Ausmass solcher Überwachungen, die mit entsprechendem finanziellem, technischem und personellem Aufwand fast flächendeckend betrieben werden. Dadurch wurden der Öffentlichkeit die Gefahren einer fast unbegrenzten und unkontrollierten Nutzung der modernen technischen Möglichkeiten bewusst.

Das Nachrichtendienstgesetz soll hier einen klaren rechtlichen Rahmen setzen, der die Anwendung solcher Mittel durch den schweizerischen Nachrichtendienst eng beschränkt, an die Verhältnismässigkeit und Notwendigkeit bindet und sie richterlichen, politischen und demokratisch legitimierten Kontrollen unterstellt. Ein vollständiger Verzicht auf solche Mittel wäre hingegen falsch. Damit würde das Feld erst recht den ausländischen Interessen überlassen, und die Schweizer Abwehr-

organe wären weiterhin nicht in der Lage, die oben erwähnten Aktivitäten auch nur ansatzweise festzustellen und aufzuklären, weil ihnen der Zugang zu den betroffenen Datenkanälen verboten bliebe.

Der Bundesrat ist deshalb der Auffassung, dass neben Anstrengungen auf internationaler diplomatischer Ebene auch wirksame eigene Aufklärungs- und Abwehrmittel notwendig sind, um die Sicherheit der Schweiz zu schützen. Dazu gehören auch Informationsbeschaffungen in Bereichen, die bisher dem schweizerischen Nachrichtendienst nicht zugänglich waren.

Erlass einer Gesamtkodifikation

Der vorliegende Gesetzesentwurf setzt den BRB vom 27. November 2009 um und stellt eine gesamtheitliche Kodifikation als Grundlage für den NDB dar. Die bisher in zwei getrennten Gesetzen enthaltenen Bestimmungen über die Inland- und die Auslandbeschaffung werden in einem einzigen Gesetz zusammengeführt.

Der Gesetzesentwurf unterscheidet nach seinem Konzept nicht mehr primär zwischen Bedrohungen aus dem Inland und aus dem Ausland, sondern zwischen gewalttätigem Extremismus mit Bezug zur Schweiz einerseits und den übrigen Bedrohungsfeldern und Aufgaben andererseits. Angesichts der heutigen Bedrohungsformen (z.B. betreffend den Terrorismus) kann die Abgrenzung zwischen dem Inland und dem Ausland oft nicht mehr klar gezogen werden.

Der Gesetzesentwurf regelt die Hauptaufgaben des NDB und enthält die Bestimmungen, die aus verfassungsrechtlichen Gründen einer formellgesetzlichen Grundlage bedürfen. Innerhalb des gesetzlichen Rahmens präzisiert der Bundesrat die Aufgabenbereiche des NDB detailliert in einem Grundauftrag, der sich nach spezifischen Schweizer Interessen sowie nach der Entwicklung der Bedrohungslage richtet.

Berücksichtigt wird auch, dass die nachrichtendienstliche Tätigkeit national und international besonderen Rahmenbedingungen unterliegt (Geheimhaltung von angewendeten Methoden, Informationen, technischen Verbindungen und Verfahren sowie Geheimhaltung der eingesetzten Quellen, Mitarbeiterinnen und Mitarbeiter sowie der eingesetzten Sensoren). Es geht insbesondere auch darum, unumgängliche Eingriffe in die Grundrechte klar zu regeln.

Behebung der Lücken und Schwächen des geltenden Rechts

Die Schwächen des geltenden Rechts sind hauptsächlich durch die Konzeption des BWIS begründet. Dieser Erlass wurde durch die damaligen Erkenntnisse im Rahmen des Berichts der parlamentarischen Untersuchungskommission über die Vorkommnisse im EJPD beeinflusst, deren öffentliche und politische Wahrnehmung teilweise bis heute Auswirkungen zeitigt.

Der Gesetzgeber nahm beim Erlass des BWIS mit dem Grundsatz, dass die Informationsbearbeitung im Vorfeld der Strafverfolgung nur sehr beschränkt erfolgen sollte, bewusst ein Sicherheitsrisiko in Kauf. Dieses sollte aber durch aufmerksame Verfolgung der Entwicklungen und periodische Neubeurteilungen der Lage gemildert werden. Die Beschaffung, Bearbeitung und Weitergabe von besonders schützenswerten Daten wurden durch ausführliche Bestimmungen geregelt und begrenzt. Damit wurde das BWIS auch den strengen Anforderungen des Bundesgesetzes vom 19. Juni 1992[10] über den Datenschutz (DSG) gerecht. Kurz nach der Inkraftsetzung

[10] SR **235.1**

des BWIS veränderte sich die Bedrohungslage mit den Terroranschlägen vom 11. September 2001 grundlegend. Verschiedene parlamentarische Vorstösse forderten in Folge eine stärkere Rolle der Staatsschutzorgane und Nachrichtendienste, einen Ausbau von deren Mitteln und Instrumentarien sowie umfassende Berichte über die Sicherheitslage. Der Bundesrat beauftragte im November 2001 das EJPD, ihm über Massnahmen zur Verbesserung der Sicherheit und zur Bekämpfung des Terrorismus Bericht und Antrag zu unterbreiten. Im Juni 2002 hiess er den Bericht «Lage- und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001»[11] gut und nahm gleichzeitig Kenntnis vom Rechtsetzungsvorhaben, das auf dem Weg einer Revision des BWIS unter anderem die Lücken im Instrumentarium zur Aufklärung von Bedrohungen schliessen sollte.

Nach mehrjährigen Vorbereitungsarbeiten legte der Bundesrat am 15. Juni 2007 dem Parlament eine Botschaft zur Änderung des BWIS (Besondere Mittel der Informationsbeschaffung; «BWIS II») vor, die die Sicherheitslage und die Lücken im präventiven Abwehrdispositiv für alle relevanten Bedrohungsbereiche aufzeigte.

Die BWIS-II-Vorlage wurde, wie vorstehend erwähnt, vom Parlament im Frühjahr 2009 an den Bundesrat zurückgewiesen. Die hauptsächlichen Lücken und Schwächen des BWIS sind deshalb bis heute unverändert geblieben.

So ist im geltenden Recht der Post- und Fernmeldeverkehr generell jeder Gefährdungsabklärung nach dem BWIS entzogen. Wo diese Informationsquelle fehlt, müssen die nachrichtendienstlichen Behörden Nachrichten mit unvergleichlich grösserem Aufwand durch getarnte menschliche Kontakte zu den entsprechenden Gruppen und Personen zu gewinnen suchen. Das Eindringen in passwortgeschützte Bereiche von Computern und Netzwerken, in welchen beispielsweise terroristische Handlungen diskutiert werden, ist zwar technisch möglich, aber – weil der Privatsphäre zurechenbar – verboten. Folge davon sind Wissenslücken bei der Früherkennung und bei der internationalen Zusammenarbeit.

Sollen Informationen über den verbotenen Nachrichtendienst gesammelt werden, so sind nach geltendem Recht nicht allgemein zugängliche Orte (z.B. Hotelzimmer) generell jeder Bedrohungsabklärung entzogen. Spioninnen und Spione nutzen diese Lücke bewusst aus; sie stehen vielfach unter diplomatischer Immunität und sind geschult, unter Tarnung Informationen zu beschaffen. Hinzu kommen Abklärungen internationaler Ermittlungsbüros, die nicht selten in (getarntem) staatlichem Auftrag handeln. Die Folge der heutigen Rechtslage ist, dass beispielsweise auch die Spionageabwehr grundsätzlich an der «Tür zum privaten Raum» endet. Dadurch entstehen gewichtige Lücken im Abwehrdispositiv.

Versuche, ausländische Massenvernichtungswaffen zu beschaffen, erfolgen über hochkomplexe internationale Netzwerke. Die Schweiz erhält dabei z.B. von dritter Seite Hinweise auf beteiligte Firmen und Finanzinstitute. Gleich wie beim Terrorismus und beim verbotenen Nachrichtendienst sind auch im Proliferationsbereich die Abklärung entsprechender Verdachtslagen durch den NDB ohne die Möglichkeit der gezielten Überwachung der Geheim- und Privatsphäre wenig erfolgversprechend.

Die Lücken und Schwächen des geltenden Rechts wurden in der Zwischenzeit auch durch eine Reihe von parlamentarischen Vorstössen thematisiert:

11 BBl **2003** 1832

- Regelungsbedarf wurde erkannt im Bereich des Einsatzes von elektronischen Aufklärungsmitteln (11.3862, Interpellation Amherd, «Verschärfung der Internetüberwachung»; 11.3471, Interpellation Malama, «Überwachung im privaten Raum. Datenschutz und Sicherheit verknüpfen»).
- Das Gleiche gilt für den Bereich der Extremismusbekämpfung (11.4076, Interpellation Eichenberger-Walther, «Künftige Regelung der Staatsschutztätigkeit»; 11.4059, Interpellation Geissbühler, «Beobachtung des Rechtsextremismus in der Schweiz»)
- Auch im Bereich des Schutzes des Finanzplatzes Schweiz wurde Regelungsbedarf erkannt (10.3028, Interpellation Fraktion der Schweizerischen Volkspartei, «Bankdatenklau. Massnahmen des Bundesrates zur Durchsetzung des Rechtsstaates»; 09.4146, Interpellation Wehrli, «Strategie für den Finanzplatz Schweiz»).

Vernehmlassungsverfahren

Stellungnahmen im Vernehmlassungsverfahren

Am 8. März 2013 verabschiedete der Bundesrat den Vorentwurf zum Nachrichtendienstgesetz und ermächtigte das VBS zur Durchführung eines Vernehmlassungsverfahrens.

Dieses dauerte vom 8. März bis zum 30. Juni 2013. Zur Teilnahme eingeladen wurden 72 Vernehmlassungsadressaten, insgesamt 68 Antworten gingen beim VBS ein (Kantone: 26, Parteien: 8, Organisationen und weitere interessierte Kreise: 34).

Grundsätzlich befürwortet wird die Vorlage von den primär für die innere Sicherheit verantwortlichen Kantonen. Diese wünschen vor allem Präzisierungen hinsichtlich der Zusammenarbeit mit dem Bund, insbesondere was die Aufsichtsfragen betrifft. Vereinzelt wird die Zustimmung unter den Vorbehalt einer neu zu schaffenden Verfassungsgrundlage gestellt.

Sämtliche grösseren politischen Parteien (mit Ausnahme der Grünen und der Piratenpartei: Ablehnung) stimmen der Vorlage mit einzelnen Vorbehalten und Änderungswünschen im Wesentlichen zu.

Bei den Dachverbänden der Wirtschaft reicht das Spektrum von Zustimmung bis Ablehnung; die von Telekommunikationskreisen geäusserte Kritik ist vor allem auf Kostenbedenken zurückzuführen, die aber mehrheitlich mit der bereits bestehenden Regelung im BÜPF zusammenhängen. Dieses befindet sich zurzeit ebenfalls in Revision, und die Kostenaspekte müssen primär dort geprüft werden.

Die weiteren interessierten Kreise halten sich in etwa die Waage, dies reicht von ganz oder tendenziell zustimmend bis zu kritisch und ganz ablehnend.

Parallel zur Auswertung der eingegangenen Stellungnahmen wurden klärende Gespräche mit der Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS) sowie mit Vertreterinnen und Vertretern der Fernmeldewirtschaft geführt, in deren Rahmen Lösungen für präzisere Regelungen gesucht wurden und einige Differenzen aus dem Weg geräumt werden konnten.

Anpassung des Vernehmlassungsentwurfs

Am 23. Oktober 2013 nahm der Bundesrat vom Ergebnisbericht[12] zum Vernehmlassungsverfahren Kenntnis und beauftragte das VBS mit der Ausarbeitung einer Botschaft bis Ende 2013.

Die wichtigsten Entscheide, welche im Rahmen der Auswertung der Vernehmlassungsergebnisse getroffen wurden, sind die folgenden:

- Auf die Schaffung einer separaten Verfassungsgrundlage für den Nachrichtendienst wird verzichtet (Ausführungen dazu in Kap. 5.1)
- Die Regelungen zur Zusammenarbeit mit den Kantonen wurden (gemeinsam mit der KKPKS) präzisiert und die kantonalen Aufsichtsrechte zur Vermeidung von Kontrolllücken erweitert (vgl. Erläuterungen der jeweiligen Artikel).
- An den Regelungen zur Kabelaufklärung wird festgehalten (vgl. Erläuterungen der jeweiligen Artikel).
- Die Regelung über den Rechtsschutz wurde klarer formuliert.

Viele Bemerkungen wurden über Ergänzungen oder Präzisierungen der Erläuterungen abgefangen.

Gesamthafte Beurteilung

Der vorliegende Gesetzesentwurf ist in mehrfacher Hinsicht von erheblicher staatspolitischer Bedeutung. Er behandelt heikle und wichtige Fragen der Abwägung von Grundrechten, so insbesondere das Verhältnis des Anspruchs der Bevölkerung auf Schutz der individuellen Freiheit, aber auch auf Schutz vor Bedrohungen, die über die von den Polizei- und Strafverfolgungsbehörden zu verfolgenden Einzelfällen hinausgehen. Im Zweckartikel stehen deshalb die Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz und die Sicherheit der Bevölkerung im Vordergrund. Der Staat wird also nicht um seiner selbst Willen geschützt, sondern es geht um die grundlegenden Zwecke, die in der Bundesverfassung definiert sind.

Das NDG geht dabei vom Grundgedanken aus, dass nachrichtendienstliche Massnahmen möglichst eng auf die tatsächlichen Bedrohungen und ihre Urheber ausgerichtet werden sollen, während der Grossteil der Bevölkerung keiner nachrichtendienstlichen Beobachtung ausgesetzt sein soll. Für die wichtigen Fälle, bei welchen es indessen um möglicherweise sehr grosse Bedrohungen der inneren oder äusseren Sicherheit und damit von sehr vielen Menschen geht, sollen auch einschneidende, aber gezielte Massnahmen zur Verfügung stehen, um die Lage frühzeitig erkennen und beurteilen zu können. Strenge gesetzliche Auflagen und wirksame Genehmigungsverfahren und Kontroll- und Aufsichtsinstrumente dienen dazu, dass diese Leitlinien eingehalten werden. Neue Beschwerderechte stellen sicher, dass richterlich geprüft wird, ob die gesetzlichen Bestimmungen eingehalten wurden.

Das NDG regelt auch die nachrichtendienstliche Auslandbeschaffung, wobei hier bei unterschiedlichen Detailregelungen zur Beschaffung dieselben Grundsätze mit Bezug auf die Verhältnismässigkeit und die Wahrung der Grundrechte gelten. Wohl spielt sich die Nachrichtenbeschaffung im und über das Ausland weitgehend in

12 www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2013 > Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport > Nachrichtendienstgesetz

einem völkerrechtlichen Graubereich ab. Sie wird jedoch von allen Staaten praktiziert, auch wenn sie umgekehrt alle Staaten unter Strafe stellen, falls die Beschaffung gegen sie gerichtet ist. Diesem Paradoxon kann sich auch das NDG nicht entziehen, stellt aber klar, dass die Beschaffung verhältnismässig sein muss. Der Kerngehalt der Grundrechte ist auch im Ausland zu wahren. Das NDG hält sich somit sowohl an die Verfassung als auch an die zwingenden völkerrechtlichen Verpflichtungen der Schweiz.

Wichtig ist auch, zu unterscheiden, dass der Nachrichtendienst keine Hilfspolizei oder kein primärer Zulieferant der Strafverfolgungsbehörden ist, sondern mit dem Fokus auf die Früherkennung von Bedrohungen eine eigenständige, sicherheitspolitische und nicht strafrechtliche Aufgabe erfüllt. Seine Berichterstattung ist deshalb auf die Verhinderung von Bedrohungen ausgerichtet und nicht auf die Verfolgung bereits geschehener Delikte.

Der Bundesrat ist der Auffassung, dass er in dieser Vorlage ausgewogene und gleichzeitig auf das Notwendige ausgerichtete Lösungen der Güterabwägungen vorgenommen hat. Das haben bereits die Ergebnisse der Vernehmlassung zu einem guten Teil bestätigt; zudem wurden weitere Präzisierungen vorgenommen. Die öffentliche politische Diskussion um das Verhältnis von Freiheit und Sicherheit, von Transparenz und notwendiger Geheimhaltung und um die Rollen von Bund und Kantonen kann mit dieser Vorlage konkret und fundiert geführt werden.

1.4 Abstimmung von Aufgaben und Finanzen

Die Gewährleistung der Sicherheit gehört zu den primären Aufgaben eines Staates. Um dessen Interessen und den Schutz der Bürgerinnen und Bürger zu wahren und um die notwendigen Massnahmen zu treffen, ist die Schweiz auf einen leistungsfähigen Nachrichtendienst angewiesen, der sicherheitsgefährdende Aktivitäten erkennt und unterbindet.

Gesellschaftliche und technische Entwicklungen sowie heutige Bedrohungen mit immer globaleren Dimensionen (z.B. Extremismus, Terrorismus, Wirtschaftskriminalität, Verbreitung atomarer oder chemischer Waffen) machen es nötig, dass diese Bedrohungen besser und früher als bisher erkannt werden und darauf rasch und wirksam reagiert werden kann. Auch der zivile Nachrichtendienst muss dabei modernste Technologien und Methoden einsetzen können.

Angesichts dieser Tatsachen beurteilt der Bundesrat die mit der Umsetzung verbundenen Kosten als vertretbar, zumal der NDB auch nach einer Aufstockung um die beantragten Stellen weit unter der Grösse der Dienste vergleichbarer europäischer Staaten bleiben wird.

1.5 Rechtsvergleich, insbesondere mit dem europäischen Umfeld

In der tabellarischen Zusammenstellung werden verschiedene Nachrichtendienstsysteme aus dem europäischen Umfeld der Schweiz in ausgewählten Punkten miteinander verglichen. Folgendes waren die Kriterien für die Auswahl der Länder:

– Deutschland und Frankreich sind bedeutende Nachbarn und haben eine ähnliche Rechtstradition wie die Schweiz.
– Analog zum NDB handelt es sich beim spanischen und beim niederländischen Dienst um fusionierte Nachrichtendienste.
– Österreich und Belgien sind in Bezug auf die Schweiz Länder von vergleichbarer Grösse.

	Deutschland *Bundesamt für Verfassungsschutz (BfV)* *Bundesnachrichtendienst (BND)*
Position in der Sicherheitsarchitektur	*BfV:* Der Inlandnachrichtendienst (zusammen mit den Landesämtern für Verfassungsschutz LfV) untersteht dem **Innenministerium**. *BND:* Der Auslandnachrichtendienst ist direkt der **Bundesregierung** unterstellt. Neben diesen beiden hat nur noch der militärische Abschirmdienst *MAD* einen nachrichtendienstlichen Status.
Aufgaben	*BfV:* – Sammeln und Auswerten von Auskünften, Nachrichten und Unterlagen in Bezug auf Bestrebungen, die gegen die freiheitliche demokratische Grundordnung oder gegen den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind; Sammeln und Auswerten von Auskünften, Nachrichten und Unterlagen in Bezug auf Bestrebungen, die durch Anwendung von Gewalt oder darauf ausgerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik gefährden oder die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind; – Spionagebekämpfung; Proliferationsabwehr; Wirtschaftsschutz; Mitwirkung bei Sicherheitsüberprüfungen von Personen aus Anlass des Geheim- und Sabotageschutzes. *BND:* – Sammeln und Auswerten von Informationen, die erforderlich sind zur Gewinnung von Erkenntnissen von aussen- und sicherheitspolitischer Bedeutung für den Staat; – Liefern von politischen, wirtschaftlichen, militärischen und wissenschaftstechnologischen Informationen über das Ausland.

Kompetenzen (Einsatz nachrichtendienstlicher Mittel)

BfV:

Der Einsatz nachrichtendienstlicher Mittel wird für das *BfV* gesetzlich klar geregelt.

Zur Erfüllung seiner Aufgaben ist es dem *BfV* unter Einhaltung von gesetzlichen Auflagen gestattet:

- Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung anzuwenden bzw. einzusetzen (z.B. Vertrauensleute, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere oder Tarnkennzeichen);
- bei Finanzinstituten, Post-, Luftfahrt- und Telekommunikationsunternehmen Informationen einzuholen;
- auf diverse vom Bund geführte Datenbanken zuzugreifen (z.B. auf das Ausländerzentralregister des Bundesamts für Migration und Flüchtlinge, die Asyldaten des Bundesamts für die Anerkennung ausländischer Flüchtlinge oder das Fahrzeugregister).

Für die Beobachtung von Organisationen und Individuen sind konkrete Anhaltspunkte für den Verdacht auf verfassungs- oder sicherheitsgefährdende Aktivitäten notwendig.

BND:

Im oder auf das Ausland angewendete nachrichtendienstliche Mittel (v.a. Erkenntnisgewinnung aus menschlichen Quellen [Human Intelligence, HUMINT] und Fernmeldeaufklärung) werden gesetzlich nicht geregelt, dafür jedoch die Aktivitäten des *BND* auf deutschem Staatsgebiet.

Er darf im Einklang mit dem Bundesdatenschutzgesetz erforderliche Informationen einschliesslich personenbezogener Daten erheben, verarbeiten und nutzen:

- um seine Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten zu schützen;
- für die Sicherheitsüberprüfung von Personen, die für ihn tätig sind oder tätig werden sollen;
- für die Überprüfung der für die Aufgabenerfüllung notwendigen Nachrichtenzugänge;
- für die Beschaffung von Informationen über Vorgänge im Ausland, die von aussen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, wenn sie nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist.

Falls zur Aufgabenerfüllung erforderlich, darf der *BND* bei Post- und Teledienstanbietern, Luftfahrtunternehmen und Kreditinstituten im Einzelfall Auskünfte über Daten einholen. Ausserdem darf er Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung (z.B. Einsatz von Vertrauensleuten oder

Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere oder Tarnkennzeichen) anwenden bzw. einsetzen.

Das *BfV* und der *BND* unterliegen bei der Post- und Telekommunikationsüberwachung dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Somit können schwerwiegende Massnahmen in diesem Bereich die Zustimmung des parlamentarischen Kontrollgremiums oder der G-10-Kommission voraussetzen.

Beide Dienste haben weder polizeiliche Befugnisse noch Weisungsbefugnisse.

Aufsicht

BfV/BND:

– Das **parlamentarische Kontrollgremium** hat zur aktiven Kontrolle das Recht auf Einsicht in Akten und Dateien der Nachrichtendienste, auf Anhörungen von Mitarbeiterinnen und Mitarbeitern, auf Besuche und im Einzelfall auf Unterstützung durch Expertinnen und Experten. Ausserdem ist die Bundesregierung verpflichtet, das Gremium über die Tätigkeiten der Nachrichtendienste zu unterrichten, ausser es liegen die Voraussetzungen vor, um die Auskunft zu verweigern, z.B. aus zwingenden Gründen des Quellenschutzes. Das Gremium nimmt auch an Entscheidungsfindungen zu Massnahmen im Bereich der sogenannten strategischen Überwachung teil.

– **Parlamentarische Untersuchungsausschüsse** können eingesetzt werden, um ernsthafte Vorfälle aus dem nachrichtendienstlichen Bereich aufzuklären sofern mindestens ein Viertel der Bundestagsabgeordneten den Antrag unterstützen. Dieses Instrument dient nicht dazu, eine kontinuierliche Kontrollfunktion auszuüben. Es besteht aber eine umfassende Aktenvorlagepflicht aller öffentlichen Stellen sowie eine Aussagepflicht für Regierungsvertreterinnen und -vertreter und Mitarbeiterinnen und Mitarbeiter der Nachrichtendienste.

– Die Nachrichtendienste werden auch im Rahmen des Artikel-10-Gesetzes kontrolliert. Das parlamentarische Gremium und die **G-10-Kommission** ergänzen sich bei der Kontrolle von Post- und Telekommunikationsüberwachungen. Daneben entscheidet die G-10-Kommission über die Zulässigkeit und Notwendigkeit von Beschränkungsmassnahmen im Rahmen der Individualkontrolle und der strategischen Kontrolle. Demnach unterrichtet sie das für den jeweiligen Nachrichtendienst verantwortliche Ministerium über beabsichtigte Massnahmen bei der strategischen Fernmeldeüberwachung. Die Kommission kann auch die gesamte Erhebung, Verarbeitung und Nutzung der durch Post- oder Telekommunikationsüberwachung erlangten personenbezogenen Daten überprüfen, nicht zuletzt durch das Recht auf Auskunft, Unterlageneinsicht und Zutritt zu allen Diensträumen.

– Das **parlamentarische Vertrauensgremium**, ist für die Kontrolle des Haushalts der Nachrichtendienste zuständig.

– Der **Bundesrechnungshof** prüft die Jahresrechnung sowie die Haushalts- und Wirtschaftsführung.

– Der **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit** überprüft sowohl beim Inland- als auch beim Auslandnachrichtendienst die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften für den Datenschutz.

Datenschutz

BfV/BND:

Der Umgang der Dienste mit personenbezogenen Daten und die Rechte der betroffenen Personen sind in der nachrichtendienstlichen Gesetzgebung geregelt. Die jeweiligen Regelungen für das *BfV* und den *BND* sind nahezu identisch.

Das *BfV* darf personenbezogene Daten speichern, verändern und nutzen, wenn konkrete Anhaltspunkte für den Verdacht auf verfassungs- oder sicherheitsgefährdende Aktivitäten vorliegen; der *BND* darf dies tun, soweit die Erfüllung seiner Aufgaben dies verlangt. Die Daten sind jedoch bei Unrichtigkeit zu berichtigen und bei Unzulässigkeit oder wenn sie nicht mehr benötigt werden, zu löschen. Dies wird bei Einzelfällen oder nach festgesetzten Fristen überprüft (*BfV*: nach fünf Jahren; *BND*: nach zehn Jahren).

Personenbezogene Daten, welche schutzwürdige Interessen von Betroffenen beeinträchtigen und für die künftige Aufgabenerfüllung nicht mehr erforderlich sind, müssen gesperrt werden.

Sofern eine betroffene Person auf einen konkreten Sachverhalt hinweisen und ein besonderes Interesse an einer Auskunft darlegen kann, erhält sie unentgeltlich Auskunft über sie betreffenden Daten.

Unter gewissen Umständen dürfen personenbezogene Daten an ausländische Behörden, an Dienststellen der Stationierungsstreitkräfte sowie an über- und zwischenstaatliche Stellen weitergeben werden. Der *BND* darf personenbezogene Daten unter gewissen Umständen von anderen deutschen Behörden beziehen.

Frankreich

Direction centrale du renseignement intérieur (DCRI)

Direction générale de la sécurité extérieure (DGSE)

Das französische Weissbuch von 2008 sieht die Erarbeitung eines gesetzlichen Rahmens für die Aktivitäten der französischen Nachrichtendienste vor, trotzdem sind ihre Tätigkeiten bisher gesetzlich kaum geregelt.

Position in der Sicherheits-architektur	*DCRI:* Der Inlandnachrichtendienst untersteht dem **Innenministerium**. *DGSE:* Der Auslandnachrichtendienst untersteht dem **Verteidigungs-ministerium**. Das Nachrichtendienstwesen in Frankreich besteht aus verschiedenen komplementären Diensten. Ausser der *DCRI* und der *DGSE* gibt es noch sechs weitere Dienste.
Aufgaben	*DCRI:* – Verhinderung und Verfolgung von Aktivitäten, die von ausländischen Mächten und Organisationen angestiftet, eingeleitet oder unterstützt werden und die die Sicherheit des Landes bedrohen; – Teilnahme an der Verhinderung und Verfolgung von Terrorakten oder Handlungen, die die Autorität des Staates, die Geheimhaltungspflicht der Landesverteidigung oder die wirtschaftlichen Interessen des Landes gefährden; – Beitrag zur Überwachung von Funk- und elektronischer Kommunikation, welche die Sicherheit des Staates gefährdet, sowie zum Kampf gegen Kriminalität im Bereich Informations- und Kommunikationstechnologie; – Teilnahme an der Überwachung von Personen, Gruppen, Organisationen und Gesellschaftsphänomenen, welche durch ihren radikalen Charakter, ihre Einstellung oder ihre Wirkungsweise die nationale Sicherheit gefährden. *DGSE:* – Suchen und Auswerten von Informationen, die für die Sicherheit Frankreichs relevant sind, für die Regierung und in Zusammenarbeit mit anderen Organisationen; – Aufdecken oder Erschweren jener Spionageaktivitäten, die ausserhalb des nationalen Territoriums gegen französische Interessen gerichtet sind (im Sinne einer vorbeugenden Massnahme). – Die *DGSE* gewährleistet dabei die notwendigen Verbindungen zu anderen relevanten Diensten und Organisationen, führt jegliche von der Regierung anvertrauten Aktionen im Rahmen ihrer Zuständigkeit aus und legt die gesammelten Informationen als Synthesen vor. – Die *DGSE* berücksichtigt dabei besonders die Terrorismusbekämpfung und den Kampf gegen die Proliferation von Massenvernichtungswaffen, allerdings auch den militärischen und den strategischen Nachrichtendienst.

Kompetenzen (Einsatz nachrichtendienstlicher Mittel)	*DCRI:* Die DCRI arbeitet mit den Regierungen der Departemente und den Präfekturen der nationalen Polizei zusammen. Ihre Kompetenzen werden gesetzlich noch nicht geregelt. *DGSE:* Die DGSE gewinnt Informationen durch sämtliche nachrichtendienstliche Methoden: HUMINT, Fernmelde- und elektronische Aufklärung (Signal Intelligence, SIGINT), Informationen aus frei verfügbaren, offenen Quellen (Open Source Intelligence, OSINT) und operationale Mittel. Sie arbeitet mit anderen französischen und ausländischen Nachrichtendiensten zusammen. Geheime Operationen durch paramilitärische Agentinnen und Agenten. Methoden und Kompetenzen werden nicht gesetzlich geregelt.
Aufsicht	*DCRI/DGSE:* – Die **parlamentarische Delegation für die Nachrichtendienste** beaufsichtigt die Tätigkeiten und Mittel. Die Delegation erhält Informationen über das Budget, die allgemeinen Tätigkeiten und die Organisation der Nachrichtendienste, jedoch nicht über die operationalen Aktivitäten, die Regierungsanweisungen, die entsprechende Finanzierung und den Austausch mit ausländischen Diensten oder internationalen Organisationen. Von den zugänglichen Informationen ausgeschlossen sind jene, die die Anonymität, die Sicherheit oder das Leben einer Person gefährden könnten oder für die Informationsgewinnung spezifische Operationsmethoden preisgeben würden. Die Arbeit der Parlamentarischen Delegation untersteht der Geheimhaltungspflicht der Landesverteidigung. Empfehlungen und Beobachtungen, Jahresbericht – Weitere Kontrollinstanzen: – **Commission nationale de contrôle des interceptions de sécurité** für die Überwachung des Abhörens von häuslicher Kommunikation; – **Commission nationale de l'informatique et des libertés** für die Kontrolle des Datenschutzes; – **Commission de vérification des fonds spéciaux** für die Zuteilung von speziellen Geldmitteln für die Nachrichtendienste.
Datenschutz	*DCRI/DGSE:* Speziell für die Nachrichtendienste wurden keine spezifischen Datenschutzauflagen festgelegt. Die Nachrichtendienste unterliegen jedoch den allgemeinen Datenschutzbestimmungen und der Kontrolle der Commission nationale de l'informatique et des libertés. Diese kontrolliert die Einhaltung des Datenschutzgesetzes und den Umgang mit personenbezogenen Daten durch die Nachrichtendienste und nimmt im Auftrag betroffener Bürge-

	rinnen und Bürger deren Recht auf Akteneinsicht wahr; dieses Recht kann im Kontext der französischen Nachrichtendienste nur auf diese indirekte Weise realisiert werden.
	Spanien *Centro Nacional de Inteligencia (CNI)*
Position in der Sicherheitsarchitektur	Das *CNI* untersteht dem **Verteidigungsministerium**. Es hat die Leitung der spanischen Nachrichtendienstgemeinschaft inne. Es wird ergänzt durch einen militärischen und weitere kleinere Nachrichten- und Informationsdienste.
Aufgaben	– Sammeln, Auswerten und Verarbeiten von Informationen im In- und Ausland, um die politischen, wirtschaftlichen, industriellen, Handels- und strategischen Interessen Spaniens zu schützen und zu fördern; – Verhinderung, Aufdeckung und Neutralisierung von Aktivitäten ausländischer Dienste, Gruppen oder Personen, welche die verfassungsmässige Ordnung, die Rechte oder Freiheiten der spanischen Bürgerinnen und Bürger, die Souveränität, die Integrität oder die Sicherheit des Staates, die Stabilität der Institutionen, die nationalen Wirtschaftsinteressen oder das Wohlergehen der Bevölkerung bedrohen, verletzen oder ein Risiko dafür darstellen; – Förderung der Beziehungen und der Zusammenarbeit mit den Nachrichtendiensten anderer Länder und internationaler Organisationen; – Sammeln, Auswerten und Interpretieren von SIGINT; – Koordination der verschiedenen Amtsstellen, die Chiffriermethoden verwenden, sowie die Gewährleistung der Sicherheit der Informationstechnologien in diesem Bereich; eine weitere Tätigkeit ist die Beschaffung von Material für die Kryptologie und die Ausbildung von Personal; – Kontrolle der Einhaltung der Regelungen zum Schutz geheimer Informationen; – Garantieren von Sicherheit und Schutz der eigenen Einrichtungen, Informationen, materiellen und personellen Mitteln.
Kompetenzen (Einsatz nachrichtendienstlicher Mittel)	Die Kompetenzen des *CNI* werden gesetzlich nur teilweise geregelt, der Einsatz nachrichtendienstlicher Mittel wird gerichtlich kontrolliert. Das *CNI* erfüllt seine Aufgaben durch das Sammeln von Informationen mit nachrichtendienstlichen Mitteln sowohl im In- als auch im Ausland. Es kann Sicherheitsuntersuchungen über Personen und Entitäten durchführen und darf dabei auf die erforderliche

	Mitarbeit von öffentlichen und privaten Organisationen und Institutionen zählen. Die nachrichtendienstlichen Mittel werden nicht eindeutig geregelt, ergeben sich jedoch aus der Erlaubnis, Mittel einzusetzen, die die Unverletzlichkeit des privaten Wohnraums oder die Vertraulichkeit des Datenverkehrs berühren (z.B. Überwachung und Abhörung). Diese Erlaubnis kann das *CNI* auf Anfrage des Direktors an den zuständigen Richter des obersten Gerichtshofs erhalten, wenn der Einsatz der Mittel zur Erfüllung der Aufgaben notwendig ist. Die Anfrage muss formell und schriftlich erfolgen und die notwendigen Massnahmen, die Umstände, die Ziele und die Gründe dieser Massnahmen spezifizieren. Ausserdem muss die Anfrage Angaben zu den betroffenen Personen und den Ort, wo die Massnahmen angewendet werden sollen, beinhalten. Die zuständige Richterin oder der zuständige Richter muss innerhalb von 72 Stunden und in dringenden Fällen innerhalb von 24 Stunden einen Entscheid fällen. Das *CNI* verfügt über Mittel zur verdeckten Ermittlung und kann von den zuständigen Behörden die für seine Missionen notwendigen Identitäten, Immatrikulationen und Ausweise erhalten. Den Agenten des *CNI* ist das Tragen von Waffen im Einklang mit den jeweiligen Bedürfnissen und den gesetzlichen Vorschriften erlaubt. Abgesehen vom Sicherheitspersonal verfügt der spanische Nachrichtendienst jedoch über keine polizeilichen Befugnisse.
Aufsicht	Das **parlamentarische Komitee für die Beaufsichtigung geheimer Fonds** ist für die parlamentarische Kontrolle zuständig. Es prüft die von der Regierung vorgegebenen Ziele und den Jahresbericht der Direktorin oder des Direktors des *CNI* über Aktivitäten und Situation bezüglich vorgegebener Ziele. Das Komitee hat nur Zugang zu Informationen, die sich nicht auf Quellen und Ressourcen des *CNI* beziehen oder die von ausländischen Nachrichtendiensten oder internationalen Organisationen stammen. Das Komitee darf zudem keine Dokumente, auch keine Kopien, an sich nehmen. Der Einsatz nachrichtendienstlicher Mittel unterliegt der **gerichtlichen Kontrolle**.
Datenschutz	Die Gesetzestexte, die sich mit dem *CNI* befassen, erwähnen weder Fragen des Datenschutzes noch verweisen sie auf ein nationales Datenschutzgesetz, an das sich der spanische Nachrichtendienst halten müsste.

	Niederlande *Algemene Inlichtingen- en Veiligheidsdienst (AIVD)*
Position in der Sicherheitsarchitektur	Der *AIVD* untersteht dem **Innenministerium**. Er wird durch den militärischen Nachrichtendienst ergänzt.
Aufgaben	– Ermittlungen zu Personen und Organisationen, die begründet im Verdacht stehen, eine ernste Gefahr für die demokratische Gesetzesordnung, die nationale Sicherheit oder andere wichtige Interessen der Niederlande darzustellen; – Überprüfung von Kandidatinnen und Kandidaten für Positionen mit Geheimhaltungsverpflichtung; – Unterstützung der Institutionen, die für die Sicherheit der privaten und staatlichen Infrastrukturen verantwortlich sind, die für den Erhalt der niederländischen Gesellschaftsstruktur lebenswichtig sind; – Ermittlungen zu Ländern im Einklang mit Aktivitäten, welche die Premierministerin oder der Premierminister, die Innenministerin oder der Innenminister und die Verteidigungsministerin oder der Verteidigungsminister zusammen in Auftrag gegeben haben; – Erstellung von Risiko- und Gefahrenanalysen zu Immobilien, Dienstleistungen und Individuen für das nationale Sicherheitssystem.
Kompetenzen (Einsatz nachrichtendienstlicher Mittel)	Die Kompetenzen des *AIVD* werden gesetzlich relativ klar geregelt, der Einsatz nachrichtendienstlicher Mittel wird für den *AIVD* durch eine Vielzahl von Auflagen im Nachrichten- und im Sicherheitsdienstgesetz reglementiert. Für die Informationsbeschaffung verfügt er über folgende Befugnisse: – Kontaktieren von sämtlichen Behörden oder Personen, die fähig scheinen, notwendige Informationen zu vermitteln; – Überwachung von Personen und Objekten mit oder ohne technische Hilfsmittel zur Aufnahme, Spurenverfolgung oder Lokalisierung; – Einsatz von verdeckten Ermittlerinnen und Ermittlern; – Durchsuchen von geschlossenen Räumen und Objekten; – Öffnen von Briefen und anderen Warensendungen ohne Einwilligung der Absenderin oder des Absenders oder der Empfängerin oder des Empfängers (braucht aber Mandat vom Bezirksgericht Den Haag); – Eindringen in Computersysteme mit oder ohne technische Instrumente oder falsche Zeichen, Passwörter oder Identitäten;

– Abhören, Aufnehmen oder Überwachen jeglicher Form von Konversation, Telekommunikation oder Datentransfer mithilfe technischer Apparate;

– Anfrage an öffentliche Telekommunikationsnetzwerkbetreiber um Informationen über eine Benutzerin oder einen Benutzer zu erhalten.

Diese Befugnisse unterliegen strikten gesetzlichen Auflagen und benötigen oft eine Weisung der zuständigen Ministerin oder des zuständigen Ministers oder der Direktorin oder des Direktors des Nachrichtendienstes.

Der *AIVD* hat keine polizeilichen Befugnisse, es ist ihm untersagt, Straftaten nachzugehen.

Aufsicht

– Ein **parlamentarisches Aufsichtskomitee über die Nachrichten- und Sicherheitsdienste** kontrolliert die Einhaltung des Nachrichten- und Sicherheitsdienstgesetzes durch den zivilen und den militärischen Nachrichtendienst.

  Alle am nachrichtendienstlichen Prozess Beteiligten sind zur Kooperation mit dem Komitee verpflichtet. Ausserdem hat das Komitee Zugang zu allen nachrichtendienstlichen Informationen und das Recht, Zeuginnen und Zeugen sowie Expertinnen und Experten zu befragen und eine Untersuchung einzuleiten.

– Der **Nationale Ombudsmann** ist für Beschwerden aus der Bevölkerung bezüglich des Verhaltens der Nachrichten- und Sicherheitsdienste zuständig. Er entscheidet über solche Beschwerden und begründet seine Position, sofern die Sicherheit und andere Interessen des Staates nicht dagegen sprechen. Anschliessend informiert er die betreffende Ministerin oder den betreffenden Minister über seinen Entscheid. Der Ombudsmann kann auch Empfehlungen abgeben. Die Ministerin oder der Minister übermittelt die Empfehlungen und die Schlüsse, die er daraus zieht, anschliessend dem niederländischen Parlament.

– Die **allgemeine Rechnungsstelle** überprüft die Ausgaben des *AIVD* für geheime Operationen und erstattet dem Parlament jährlich Bericht darüber.

– Die für die Nachrichten- und Sicherheitsdienste verantwortlichen Ministerinnen und Minister berichten dem Parlament einmal jährlich über die Aktivitäten des *AIVD*.

Datenschutz

Der *AIVD* darf personenbezogene Daten einer Person nur in folgenden Fällen verwenden oder bearbeiten:

– wenn ein ernsthafter Verdacht besteht, dass diese Person eine Gefahr für die demokratische Gesetzesordnung, die Sicherheit oder andere lebenswichtige Interessen des Landes darstellt;

– wenn die Person ihr Einverständnis zu einer Sicherheitsüberprüfung gegeben hat;

– wenn dies im Rahmen von Nachforschungen über andere Länder erforderlich ist;
– wenn die Informationen von einem anderen Nachrichten- oder Sicherheitsdienst beschafft wurden;
– wenn die Daten für den Dienst notwendig sind, damit dieser seine Pflichten erfüllen kann;
– wenn die Person beim Dienst angestellt ist oder war; oder
– wenn die Daten zur Erstellung von Risikoanalysen notwendig sind.

Wenn personenbezogene Daten für den Zweck, für den sie gesammelt wurden, keine Bedeutung mehr haben, müssen sie entfernt werden. Auch Informationen, die sich als falsch erweisen oder unrechtmässig verarbeitet wurden, werden korrigiert oder entfernt.

Ministerinnen und Minister, andere relevante Personen und Behörden, die relevanten Nachrichten- und Sicherheitsdienste anderer Länder sowie die relevanten internationalen Sicherheits-, SIGINT- und Nachrichtendienstorganisationen dürfen über die vom *AIVD* verarbeiteten Informationen in Kenntnis gesetzt werden.

Bezüglich des Rechts, persönliche Daten einzusehen, muss die zuständige Ministerin oder der zuständige Minister die Antragsstellerin oder den Antragssteller sobald als möglich informieren, welche personenbezogenen Daten durch oder für den Dienst verarbeitet wurden. Daraufhin hat die Antragsstellerin oder der Antragssteller das Recht, die Daten einzusehen.

Österreich

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)

Heeresnachrichtenamt (HNaA)

Position in der Sicherheitsarchitektur

BVT:

Der Inlandnachrichtendienst untersteht als Teil der Sicherheitspolizei der Generaldirektion für öffentliche Sicherheit im **Bundesministerium für Inneres**.

Das *BVT* wird unterstützt von neun Landesämtern für Verfassungsschutz und Terrorismusbekämpfung.

HNaA:

Der strategische Auslandnachrichtendienst untersteht innerhalb des **Bundesministeriums für Landesverteidigung und Sport** der Generalstabschefin oder dem Generalstabschef.

	Neben dem Inland- und dem Auslandnachrichtendienst gibt es als einzigen zusätzlichen Dienst das Abwehramt in der Funktion des militärischen Nachrichtendienstes.
Aufgaben	*BVT:* – Informationsbeschaffung, Ermittlung und Analyse in den Bereichen Terrorismus, Extremismus, Spionageabwehr, illegaler Waffenhandel und Proliferation; – Personen- und Objektschutz für Organwalter verfassungsmässiger Einrichtungen; – Schutz von Vertreterinnen und Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtsobjekte; – Schutz kritischer Infrastrukturen; – Sicherheitsüberprüfungen. *HNaA:* Nachrichtendienstliche Aufklärung: Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder andere zwischenstaatliche Einrichtungen in Bezug auf militärische und damit zusammenhängende sonstige Tatsachen, Vorgänge und Vorhaben
Kompetenzen (Einsatz nachrichtendienstlicher Mittel)	Der Einsatz nachrichtendienstlicher Mittel wird für beide Dienste gesetzlich klar geregelt. *BVT:* Das *BVT* gewinnt seine Informationen durch die Auswertung von OSINT sowie nicht offener Quellen. In diesem Rahmen (erweiterte Gefahrenforschung) verfügt es über folgende Befugnisse: – Beobachtung von Gruppierungen, wenn aufgrund des Umfelds und der Entwicklung mit einer ernsthaften Gefahr für die öffentliche Sicherheit und mit damit verbundener Kriminalität, insbesondere mit religiös oder weltanschaulich motivierter Gewalt, zu rechnen ist; – verdeckter Einsatz von Erkennungsgeräten für Kraftfahrzeugkennzeichen und der offene Einsatz von Bild- und Tonaufzeichnungsgeräten an Kriminalitätsbrennpunkten; – verdeckter Einsatz von Bild- und Tonaufzeichnungsgeräten und die Übermittlung privater Bild- und Tonaufzeichnungen an Sicherheitsbehörden unter bestimmten Voraussetzungen; – Observationen und der Einsatz verdeckter Ermittlerinnen und Ermittler.

Je nach Eingriffsintensität setzt die Verwendung der nachrichtendienstlichen Mittel die Verständigung der oder des Rechtsschutzbeauftragten des Bundesministeriums für Inneres bzw. die vorgängige Ermächtigung durch diese oder diesen voraus.

Das *BVT* ist ein Polizeidienst und hat somit als Teil der Sicherheitspolizei dem Sicherheitspolizeigesetz entsprechende polizeiliche Befugnisse.

HNaA:

Laut dem Militärbefugnisgesetz hat das *HNaA* folgende Befugnisse zum Zweck der nachrichtendienstlichen Aufklärung:

- Einholen von Auskünften bei Personen, bei Organen der Gebietskörperschaften und anderer Körperschaften des öffentlichen Rechts, bei den durch diese Körperschaften betriebenen Stiftungen, Anstalten und Fonds sowie bei Betreibern öffentlicher Telekommunikationsdienste;
- Datenermittlung durch Observation, wenn ansonsten die Aufgabenerfüllung verhindert oder erheblich behindert würde;
- verdeckte Ermittlung, wenn dies im Interesse der nationalen Sicherheit, insbesondere im Interesse der Gewährleistung der Einsatzbereitschaft des Bundesheeres, dringend erforderlich ist und ansonsten die Aufgabenerfüllung der Aufklärung verhindert würde;
- Datenermittlung mit Bild- und Tonaufzeichnungsgeräten, wenn dies im Interesse der nationalen Sicherheit, insbesondere im Interesse der Gewährleistung der Einsatzbereitschaft des Bundesheeres, unerlässlich ist und ansonsten in grösserem Umfang die Aufgabenerfüllung der Aufklärung verhindert würde.

Vor einer Datenermittlung durch Observation, verdeckte Ermittlung oder Bild- und Tonaufzeichnungsgeräte muss das *HNaA* die oder den Rechtsschutzbeauftragten zur Prüfung der Rechtmässigkeit von Massnahmen der nachrichtendienstlichen Aufklärung oder Abwehr unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis setzen; ferner muss das *HNaA* die Bundesministerin oder den Bundesminister für Landesverteidigung verständigen. Eine solche Ermittlung darf erst aufgenommen werden, wenn eine entsprechende Zustimmung der oder des Rechtsschutzbeauftragten vorliegt. Würde aber bei weiterem Zuwarten ein nicht wiedergutzumachender, schwerer Schaden für die nationale Sicherheit, insbesondere für die Einsatzbereitschaft des Bundesheeres oder für die Sicherheit von Menschen, eintreten, so kann die Ermittlung sofort nach Kenntnisnahme durch die rechtsschutzbeauftragte oder den Rechtsschutzbeauftragten aufgenommen und durchgeführt werden, sofern Letztere oder Letzterer diese nicht durch einen Einspruch beendet.

Aufsicht

BVT:

- Kontrolle im Rahmen des parlamentarischen Interpellationsrechts.
- Kontrolle durch den **ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Massnahmen zum Schutz der verfassungsmässigen Einrichtungen und ihrer Handlungsfähigkeit**. Dieser ist für die Überprüfung der gesetzmässigen Aufgabenerfüllung durch das *BVT* zuständig. Er ist befugt, vom Bundesminister für Inneres Auskünfte zu verlangen und Einsicht in Unterlagen zu erhalten.
- Eher administrative Kontrolle durch den **Rechnungshof** und die **Volksanwaltschaft**.
- Kontrolle durch den **Rechtsschutzbeauftragten des Bundesministeriums für Inneres**. Im Rahmen der speziellen Befugnisse des *BVT* reicht seine Einbindung je nach Eingriffsintensität von der blossen Kenntnisnahme bis zur vorherigen Ermächtigung zu Massnahmen. Er erstellt jährlich einen Bericht über seine Aufgabenerfüllung.
- Kontrolle durch den **Menschenrechtsbeirat**. Dieser berät die Bundesministerin oder den Bundesminister für Inneres bei Fragen bezüglich der Wahrung der Menschenrechte und beaufsichtigt in dieser Funktion auch das *BVT*. Dieses ist verpflichtet, ihn bei seinen Tätigkeiten zu unterstützen, zudem stellt ihm die Bundesministerin oder der Bundesminister die zur Erfüllung der Aufgaben notwendigen Mittel zur Verfügung.

HNaA:

- Kontrolle im Rahmen des parlamentarischen Interpellationsrechts.
- Kontrolle durch den s**tändigen Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Massnahmen zur Sicherung der militärischen Landesverteidigung**. Dieser kann vom *HNaA* alle einschlägigen Auskünfte und Unterlagen verlangen. Im Sinne des Quellenschutzes ist er jedoch nicht befugt, Auskünfte oder Unterlagen – insbesondere über Quellen – zu verlangen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden könnte.
- Kontrolle durch **die Rechtsschutzbeauftragte oder den Rechtsschutzbeauftragten zur Prüfung der Rechtmässigkeit von Massnahmen der nachrichtendienstlichen Aufklärung oder Abwehr**. Diese oder dieser ist für die Bewilligung und Kontrolle des Einsatzes nachrichtendienstlicher Mittel zuständig. Ihr oder ihm ist jederzeit Einsicht in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren; ausserdem sind ihr oder ihm die erforderlichen Auskünfte zu erteilen.

	Dies gilt jedoch nicht für Auskünfte und Unterlagen zur Identität von Personen oder zu Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden könnte. Es muss ihr oder ihm ausserdem jederzeit möglich sein, die Durchführung der von ihm zu kontrollierenden Massnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus überwacht die oder der Rechtsschutzbeauftragte die Einhaltung der Pflicht zur Richtigstellung oder Löschung gemäss den datenschutzrechtlichen Bestimmungen. Einmal jährlich erstattet sie oder er Bericht über ihre oder seine Tätigkeiten. *BVT/HNaA:* Kontrolle durch die **Datenschutzkommission**. Diese ist im Rahmen des Datenschutzgesetzes für den Rechtsschutz einer natürlichen Person zuständig, falls ein Verdacht auf Verstösse gegen das Grundrecht auf Datenschutz vorliegt. Sie befindet über Beschwerden wegen Verdachts auf Verletzung der Rechte auf Auskunft, Geheimhaltung, Richtigstellung oder Löschung.
Datenschutz	*BVT:* Der Umgang mit personenbezogenen Daten und die Rechte der betroffenen Personen sind durch das Sicherheitspolizeigesetz geregelt. Personenbezogene Daten dürfen ermittelt und verwendet werden, soweit diese zur Aufgabenerfüllung erforderlich sind. Die Daten dürfen auch von Betreibern öffentlicher Telekommunikationsdienste oder anderen Anbietern verlangt werden. Unrichtige oder unrichtig ermittelte Daten oder nicht mehr benötigte personenbezogene Daten müssen richtiggestellt oder gelöscht werden. Verarbeitete personenbezogene Daten müssen überprüft werden, sobald sie sechs Jahre unverändert geblieben sind. Betroffene Personen haben das Recht, zu den über sie ermittelten personenbezogenen Daten unentgeltlich Auskunft zu erhalten. Das *BVT* muss jedoch keine Auskunft erteilen, wenn dies zum Schutz der Auskunftswerberin oder des Auskunftswerbers notwendig ist oder wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen (z.B. der Schutz der verfassungsmässigen Einrichtungen Österreichs), der Auskunftserteilung entgegenstehen. *HNaA:* Im Militärbefugnisgesetz sind keine speziellen Regelungen zum Datenschutz vorgesehen, es verweist aber auf das Datenschutzgesetz. Das Auskunftsrecht entspricht demjenigen des BVT.

Belgien

Sûreté de l'Etat (SE)

Service générale du renseignement et de la sécurité des Forces armées (SGRS)

In Belgien ist die *SE* zivil, der *SGRS* militärisch ausgerichtet. Beide sind sowohl für das In- als auch für das Ausland zuständig, allerdings liegt der Schwerpunkt der *SE* im Inland, der *SGRS* konzentriert sich eher auf das Ausland.

Position in der Sicherheitsarchitektur

SE:

Der zivile Nachrichtendienst untersteht grundsätzlich **der Justizministerin oder em Justizminister**, in Fragen der öffentlichen Sicherheit und des Personenschutzes ist allerdings auch **die Innenministerin oder der Innenminister** zuständig.

SGRS:

Der militärische Nachrichtendienst **untersteht der Verteidigungsministerin oder dem Verteidigungsminister**.

Auch der Zolldienst und die Polizei beschäftigen sich mit der nachrichtendienstlichen Informationsbeschaffung; sie sind aber keine eigentlichen Nachrichtendienste und unterstehen daher nicht den entsprechenden Gesetzen.

Die Nachrichtendienste kooperieren sowohl miteinander als auch mit ausländischen Diensten und können die Justiz- und Administrativbehörden unterstützen.

Aufgaben

SE:

- Suche, Analyse und Bearbeitung von Informationen über Aktivitäten, welche die innere Sicherheit des Staates oder das Weiterbestehen der demokratischen oder verfassungsmässigen Ordnung, die äussere Sicherheit des Staates oder internationale Beziehungen, das wissenschaftliche oder wirtschaftliche Potenzial oder alle anderen fundamentalen Interessen des Landes bedrohen oder bedrohen könnten (Spionage, Terrorismus, Extremismus, Proliferation von Massenvernichtungswaffen, schädliche sektiererische oder kriminelle Organisationen, Einmischung);
- Sicherheitsüberprüfung;
- Personenschutz;
- andere Aufgaben nach Gesetz.

SGRS:

- Suche, Analyse und Bearbeitung von Informationen über Aktivitäten, welche die Integrität des nationalen Territoriums, die militärischen Verteidigungspläne, die Ausführung der Aufgaben der Streitkräfte, die Sicherheit von belgischen Staatsan-

gehörigen oder andere fundamentale Interessen des Landes bedrohen oder bedrohen könnten; Information der zuständigen Ministerinnen oder Minister;

- Beratung der Regierung zur Aussen- und Verteidigungspolitik;
- Gewährleistung der militärischen Sicherheit des Personals des Verteidigungsministeriums, der militärischen Einrichtungen, der Waffen, der Pläne, der Informatiksysteme, der Kommunikation und anderer militärische Objekte;
- Geheimhaltungsschutz;
- Sicherheitsüberprüfung.

Kompetenzen (Einsatz nachrichtendienstlicher Mittel)

Der Einsatz nachrichtendienstlicher Mittel wird für beide Dienste gesetzlich klar geregelt.

SE/SGRS:

Gemäss Gesetz dürfen die Dienste personenbezogene Informationen suchen, sammeln, erhalten und bearbeiten, sofern dies zur Erfüllung ihrer Aufgaben notwendig ist. Dazu können sie auf Justizbehörden, Funktionärinnen oder Funktionäre und Beamtinnen und Beamte des öffentlichen Dienstes sowie auf jegliche Personen oder Organisationen aus dem privaten Sektor zur Informationsgewinnung zurückgreifen, in öffentlich zugängliche Räume und Orte eindringen; die Dienste dürfen Hotels und andere Wohnunterkünfte besuchen sowie menschliche Quellen verwenden.

Wenn diese gewöhnlichen Methoden zur Informationsgewinnung nicht ausreichen, so können die beiden Dienste auch sogenannte spezifische oder aussergewöhnliche Methoden anwenden.

Spezifische Methoden:

- Beobachtung mit technischen Hilfsmitteln in öffentlich zugänglichen öffentlichen oder privaten Räumen oder die Beobachtung mit oder ohne technische Hilfsmittel von privaten Räumen, die für die Öffentlichkeit nicht zugänglich sind;
- Kontrolle von öffentlichen Räumen und öffentlich zugänglichen Privaträumen sowie von sich darin befindlichen geschlossenen Objekten mit technischen Hilfsmitteln;
- Identifizierung der Absenderin oder des Absenders oder der Empfängerin oder des Empfängers einer Postsendung oder der Inhaberin oder des Inhabers eines Postfachs;
- Identifizierung der Abonnentin oder des Abonnenten oder der üblichen Benutzerin oder des üblichen Benutzers eines elektronischen Kommunikationsdienstes oder des verwendeten elektronischen Kommunikationsmittels;
- Orten der Anrufdaten von elektronischen Kommunikationsmitteln und die Lokalisierung des Ursprungs oder des Ziels von elektronischer Kommunikation.

Diese Methoden dürfen erst dann angewendet werden, wenn die für die Überwachung und teilweise auch Bewilligung der Methoden geschaffene Administrativkommission darüber vom Direktor des jeweiligen Dienstes in Kenntnis gesetzt wurde.

Aussergewöhnliche Methoden:

- Beobachtung und Kontrolle von nicht-öffentlich zugänglichen Privaträumen;
- Erschaffung und Verwendung einer juristischen Person zur Unterstützung von operationalen Aktivitäten und Verwendung von Nachrichtendienstagentinnen und -agenten;
- Öffnen und Kenntnisnahme von Post;
- Sammeln von Daten über Bankkonten und Banktransaktionen;
- Eindringen in ein Informatiksystem;
- Abhören und Aufnehmen von Kommunikation.

Diese Methoden dürfen grundsätzlich erst angewendet werden, wenn sie von der dafür zuständigen Administrativkommission bewilligt worden sind.

Die belgischen Nachrichtendienste können die Justizbehörden unterstützen, haben aber selber keine polizeilichen Befugnisse (zumindest äussert sich das Gesetz nicht dazu).

Aufsicht

SE/SGRS:

- **Ständiger Kontrollausschuss für Nachrichten- und Sicherheitsdienste** (parlamentarische Kontrollinstanz): beaufsichtigt die Nachrichtendienste und kann Untersuchungen durchführen (dazu verfügt er über Akteneinsicht und kann Vorladungen, Durchsuchungen und Beschlagnahmungen veranlassen).
- **Administrativkommission**: überwacht die Anwendung der spezifischen und aussergewöhnlichen nachrichtendienstlichen Methoden.
- **Bundesombudsmann**: zuständig für Beschwerden von Einzelpersonen, kann Untersuchungen durchführen und Einsicht in Akten nehmen, es besteht aber keine Verpflichtung, geheime Informationen an ihn weiterzugeben.
- **Datenschutzkommission**: prüft im Auftrag der Bürgerinnen und Bürger die von den Diensten erstellten personenbezogenen Informationen, kann aber nur Empfehlungen abgeben und darf über den Inhalt der Akten keine Auskunft geben.

Datenschutz

SE/SGRS:

Für die *SE* und den *SGRS* gelten die gleichen Regelungen. Der Umgang der Dienste mit personenbezogenen Daten und die Rechte der betroffenen Personen sind in der nachrichtendienstlichen Gesetzgebung geregelt.

Personenbezogene Informationen und Daten können gesucht, gesammelt, erhalten und bearbeitet werden. Auch können sie an bestimmte Personen, Behörden, Polizeidienste oder alle anderen kompetenten Instanzen weitergegeben werden, sofern diese Gegenstand einer Bedrohung sind oder falls die personenbezogenen Informationen für die Ausführung ihrer Aufgaben nötig sind. Diese Daten dürfen nur so lange aufbewahrt werden, wie sie für den Zweck, für den sie aufgenommen wurden, notwendig sind, mit Ausnahme der Daten die vom Staatsarchiv als historisch bedeutend eingestuft werden. Die Vernichtung erfolgt erst nach Ablauf einer auf die letzte Bearbeitung der Daten bezogenen Frist, die von der Königin oder vom König festgelegt wird.

Die Bürgerinnen und Bürger haben kein Einsichtsrecht in die sie betreffenden personenbezogenen Akten, sie müssen sich an die Datenschutzkommission wenden.

1.6 Umsetzung

Für die Umsetzung der Massnahmen kann beinahe vollumfänglich auf die bestehenden eidgenössischen Strukturen (NDB, Bundesverwaltungsgericht, Dienst für die Überwachung des Post- und Fernmeldeverkehrs, Schweizer Vertretungen usw.) und kantonalen Strukturen (kantonale Polizei- und Sicherheitsbehörden) aufgebaut werden.

2 Erläuterungen zu einzelnen Artikeln

Vorbemerkung zum Begriff Bedrohung:

Der Begriff «Bedrohung» setzt nach der Definition im sicherheitspolitischen Bericht des Bundesrates *«einen Willen voraus, die Schweiz oder ihre Interessen zu schädigen oder zumindest eine solche Schädigung in Kauf zu nehmen»*. Der Begriff «Gefahr» setzt demgegenüber nach der Definition des Bundesrates keinen Willen zur Schädigung voraus (z.B. Naturgefahren und technische Gefahren)[13].

Der vorliegende Gesetzesentwurf verwendet zur klaren Unterscheidung von den Naturgefahren den Begriff «Bedrohung», auch wenn einzelne sicherheitspolitische Entwicklungen, die in den Aufgabenbereich des Nachrichtendienstes gehören, nicht bzw. noch nicht direkt gegen die Schweiz gerichtet sind oder eine solche Entwicklung gar geeignet sein kann, eine Bedrohung zu verhindern oder abzuwenden.

Ingress

Gestützt auf die neuere Praxis der Gesetzgebung verzichtet der Ingress auf die Erwähnung der verfassungsinhärenten Kompetenz des Bundes zur Gesetzgebung zur Wahrung der inneren oder äusseren Sicherheit. Nach aktueller Auffassung ist diese Regelungskompetenz in Artikel 173 Absatz 2 der Bundesverfassung enthalten

13 BBl **2010** 5133, hier 5146

(Behandlung von Geschäften durch die Bundesversammlung, die in die Zuständigkeit des Bundes fallen und keiner anderen Behörde zugewiesen sind).

Aus dieser Kompetenz leitet sich u. a. die (partielle) Befugnis des Bundes ab, über die Aufgaben der Kantone bzw. der kantonalen Vollzugsbehörden im Bereich der inneren Sicherheit zu legiferieren. Wir verweisen dazu auf die Ausführungen zu Artikel 9 (Kantonale Vollzugsbehörden) und 81 (Vollzug durch Kantone).

Art. 1 Gegenstand

Diese Bestimmung fasst den Regelungsumfang des Gesetzestextes zusammen.

Art. 2 Zweck

Die Einführung einer Zweckbestimmung erscheint im Hinblick auf die Bedeutung des vorliegenden Gesetzesentwurfs als Gesamtkodifikation für den Nachrichtendienst der Schweiz als angebracht. Der Artikel übernimmt Elemente des heutigen BWIS. Er definiert die Zwecke, an welchen sich letztlich die nachrichtendienstlichen Tätigkeiten ausrichten, und ist damit nicht kompetenzbegründend, sondern wirkt als Leitlinie für den Vollzug des Gesetzes.

Art. 3 Einsatz in besonderen Lagen

Das NDG regelt die Wahrung wesentlicher Landesinteressen im sicherheitspolitischen Bereich. Artikel 3 soll es dem Bundesrat ermöglichen, den NDB in besonderen Lagen mit der Informationsbeschaffung und -auswertung sowie gegebenenfalls mit operativen Tätigkeiten zu beauftragen, die über den ordentlichen gesetzlichen Auftrag des NDB hinausgehen. Hierzu ist ein Beschluss des Bundesrates nach Artikel 70 notwendig. Der Grundauftrag des Bundesrates (Art. 69 Abs. 1 Bst. a) oder die von ihm erlassene Beobachtungsliste (Art. 71) genügen nicht. Der NDB darf also nicht von sich aus oder aufgrund der ordentlichen Führungsinstrumente Grundauftrag und Beobachtungsliste zur Wahrung wesentlicher Landesinteressen nach Artikel 3 tätig werden. Mit dem Beschluss des Bundesrates stehen dem NDB keine besonderen Kompetenzen zu, die über das NDG hinausgehen. Für die Beschaffungstätigkeiten gelten somit die gesetzlichen Regeln, insbesondere für die Anwendung genehmigungspflichtiger Massnahmen (Art. 25 ff.), die nach dem normalen Verfahren zu beantragen und zu begründen sind. Der Bundesrat kann hingegen in seinem Beschluss Auflagen für die Tätigkeit des NDB machen, indem er z.B. die Aufklärungstätigkeit auf das Ausland beschränkt oder bestimmte Beschaffungsmassnahmen – beispielsweise genehmigungspflichtige – ausschliesst.

In der Regel wird es bei der Anrufung solcher wesentlicher Landesinteressen nach Artikel 3, die im allgemeinen gesetzlichen Auftrag des NDB nicht enthalten sind, um die Auslandaufklärung gehen. Diese wesentlichen Landesinteressen müssen dabei in die verfassungsmässige Kompetenz des Bundes fallen. Möglich wäre auch, dass ein oder mehrere Kantone ein Gesuch für einen Einsatz des NDB zur Wahrung solcher Landesinteressen stellen, die primär in der verfassungsmässigen Kompetenz der Kantone liegen, aber bei ihrer Bedrohung ein nationales Interesse begründen können. Der Gesetzesentwurf nennt als weitere wesentliche Landesinteressen den Schutz der verfassungsrechtlichen Grundordnung (soweit dies über den in Art. 6 definierten Auftrag des NDB hinausgeht), die Unterstützung der schweizerischen Aussenpolitik (z.B. bei aussenpolitischen Krisenlagen, heiklen Verhandlungen oder

diplomatischen Drucksituationen) und den Schutz des Werk-, Wirtschafts- und Finanzplatzes (z.B. bei wirtschaftspolitisch motivierten Druckausübungen gegen bestimmte Wirtschaftszweige von nationaler Bedeutung).

Sollten für die Erfüllung eines solchen Einsatzes besondere personelle oder finanzielle Ressourcen benötigt werden, müsste sie der Bundesrat dem NDB mit demselben Beschluss zuweisen. Die Budgethoheit der eidgenössischen Räte bleibt dabei vorbehalten.

Artikel 3 schränkt die Kompetenz des Bundesrates zum Erlass von Verordnungen, die sich auf die Artikel 184 Absatz 3 und 185 Absatz 3 der Bundesverfassung abstützen, nicht ein (vgl. auch Art. 7*a*–7*d* des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[14], RVOG).

Art. 5 Grundsätze der Informationsbeschaffung

Die Hauptaufgabe des Nachrichtendienstes besteht im Beschaffen und Beurteilen von Informationen und deren Weitergabe in Form von nachrichtendienstlichen Produkten an berechtigte Empfänger sowie in der Umsetzung der Erkenntnisse in präventive operative Leistungen, die der Verringerung der Bedrohungen der Sicherheit dienen. Deshalb definiert der Gesetzesentwurf in Artikel 5 Grundsätze für die Informationsbeschaffung, die für die Anwendung aller weiterer Bestimmungen Gültigkeit haben. Adressat ist vorab der NDB als Vollzugsbehörde des Bundes, nachgelagert aber auch die Vollzugsbehörden der Kantone, welche in direktem Vollzug des NDG oder im besonderen Auftrag des NDB tätig werden.

Die Inhalte der einzelnen Absätze werden in weiteren Bestimmungen des Gesetzes teilweise detaillierter geregelt.

Absatz 1 verweist darauf, dass der Nachrichtendienst sowohl aus öffentlichen als auch aus nicht öffentlichen Quellen Informationen beschafft. Die Kenntnis der öffentlich zugänglichen Quellen (vgl. Art. 13) ist dabei wichtig, um beurteilen zu können, welche Informationen mit nachrichtendienstlichen Mitteln zu beschaffen, zu bestätigen oder allenfalls zu widerlegen sind.

Absatz 2 verweist auf das in Kapitel 3 geregelte System der genehmigungsfreien und der genehmigungspflichtigen Massnahmen. Die genehmigungsfreien Beschaffungsmassnahmen (Art. 13 ff.) werden vom NDB in eigener Verantwortung angewendet und bedürfen keiner Bewilligung (z.B. Beobachtungen im öffentlichen Raum). Sie entsprechen in etwa dem heutigen Katalog nach Artikel 14 Absatz 2 BWIS.

Genehmigungspflichtige Beschaffungsmassnahmen (Art. 25 ff.) sind nur in den vom Gesetz vorgesehenen Fällen anwendbar und setzen eine Genehmigung durch das Bundesverwaltungsgericht sowie die Freigabe durch die Chefin oder den Chef des VBS voraus.

Absatz 3 verdeutlicht die Anwendung des allgemeinen Verhältnismässigkeitsprinzips für den Nachrichtendienst: Kerngedanke dieses Prinzips ist ein angemessenes Verhältnis zwischen dem angestrebten Zweck und dem zu seiner Erreichung notwendigen Grundrechtseingriff. So schreibt es dem NDB vor, jeweils die mildeste Massnahme zu ergreifen, die voraussichtlich am wenigsten in die Grundrechte der

[14] SR **172.010**

betroffenen Person eingreift, um seinen Auftrag zu erfüllen. Kann man eine benötigte Information mit einer genehmigungsfreien Massnahme beschaffen, so ist diese einer genehmigungspflichtigen vorzuziehen.

Absatz 4 ist notwendig, um den allgemeinen datenschutzrechtlichen Grundsatz aufzuheben, dass Personendaten nur so beschafft werden sollen, dass es für die betroffene Person erkennbar ist (Art. 4 Abs. 4 DSG). Die Regelung entspricht den heutigen Artikeln 5 Absatz 1 ZNDG und 14 Absatz 1 BWIS. Wären Beschaffung und Bearbeitung für die betroffenen Personen erkennbar, würde dies den Zweck der Datenbearbeitung in der Regel vereiteln. Hingegen besteht ein Auskunftsrecht, das in den Artikeln 62 ff. geregelt ist.

Die *Absätze 5–8* übernehmen sinngemäss bestehende und bewährte Grundsätze des Schutzes der politischen Betätigung vor nachrichtendienstlicher Beobachtung und deren Ausnahmen aus dem BWIS. In der Vernehmlassung waren vereinzelt Verschärfungen dieser Bestimmungen gefordert worden. Der Bundesrat hält indessen das erst 2001 aufdatierte heutige System für angemessen. Das NDG behält dieses bei und gewährleistet damit den gleichen Schutz, wie ihn das BWIS für die nachrichtendienstliche Bearbeitung von Vorgängen im Inland gewährleistet. Für das Ausland wäre ein solcher Vorbehalt indessen nicht sinnvoll, da sonst die Beobachtung und Beurteilung von machtpolitischen Entwicklungen praktisch verunmöglicht würde.

Als Beispiele für das missbräuchliche Ausüben von Grundrechten nach Absatz 6 zu sicherheitsgefährdenden Tätigkeiten seien angeführt:

– Ein Verein, der zum Zweck der Religionsausübung besteht, betreibt ein Versammlungslokal für seine Mitglieder. Regelmässig hält sich dort eine Person auf die versucht, Mitglieder dieses Vereins zu überzeugen, sich dem bewaffneten religiösen Kampf im Ausland anzuschliessen oder im Ausland an einer Ausbildung zum bewaffneten Kampf teilzunehmen. Die nachrichtendienstliche Aufklärung und Datenbearbeitung bezieht sich dann auf diese Person, nicht aber auf die Mitglieder des Vereins im Allgemeinen.
– Eine Gruppe von Personen einer ethnischen Minderheit, die in ihrem Heimatland den bewaffneten Kampf gegen die Regierung führt, betreibt in der Schweiz ein Lokal für vordergründig kulturelle Zwecke. Ein Folkloreabend mit Musikdarbietungen dient aber nicht dem angekündigten Zweck, sondern als Märtyrergedenkveranstaltung mit Rednern, die den bewaffneten Kampf propagieren und zu diesem Zweck Geld sammeln.

Die *Absätze 6 und 7* entsprechen den 2012 in Kraft getretenen präzisierenden Bestimmungen zu Artikel 3 BWIS. Bei einer Löschung der Daten gilt die Anbietepflicht an das Bundesarchiv. Nicht archivwürdige Daten werden definitiv vernichtet.

Absatz 8 stellt klar, dass über Organisationen und Gruppierungen der Beobachtungsliste nach Artikel 71 alle für die Bedrohungsbeurteilung relevanten Informationen bearbeitet werden dürfen. Diese Bestimmung befand sich bisher im BWIS in den Regelungen zur Beobachtungsliste, wo sie gewisse Unklarheiten über ihre Anwendung verursachte. Mit der neuen systematischen Einordnung wird dies vermieden.

Der NDB trägt primär präventiv zur Sicherheit des Landes bei. Er kann aber auch mit seinen speziellen Mitteln andere Bundesstellen bei der Durchführung ihrer Aufgaben unterstützen (vgl. Art. 68).

Die präventive Tätigkeit des NDB ist klar von der repressiven Tätigkeit der Strafverfolgungsbehörden abzugrenzen. Der NDB hat den primären Auftrag, sicherheitspolitische Bedrohungen gegen die Schweiz frühzeitig zu erkennen und darüber vor allem zuhanden der zuständigen Behörden Bericht zu erstatten. So sollen Risiken minimiert werden. Der NDB nimmt aber keine polizeilichen oder strafprozessualen Aufgaben wahr (z.B. Ermittlungen, Festnahmen, usw.). Nachrichtendienst und Strafverfolgung ergänzen sich somit, sind aber nicht die Vorstufe der jeweils anderen Instanz. Sie unterstehen deshalb auch getrennten Aufsichtsbereichen (Nachrichtendienst durch die Politik, Strafverfolgung durch die Gerichte). Daher muss der gegenseitige Informationsaustausch zwischen dem NDB und den Strafverfolgungsbehörden klar geregelt werden.

Art. 6 Aufgaben des NDB

Das Gesetz erwähnt in *Absatz 1* nur den NDB als vollziehende Behörde. Die Aufgabenbereiche nach Buchstabe a gelten jedoch auch für den Vollzug in den Kantonen (vgl. Art. 81). Sie entsprechen inhaltlich den vom BWIS bekannten sachlichen Zuständigkeitsbereichen. Ergänzt werden sie durch die ausdrückliche Erwähnung der Angriffe auf kritische Infrastrukturen, welche durch die technische Entwicklung seit dem Erlass des BWIS eine neue Bedeutung erhalten haben. Wenn solche Angriffe z.B. mit Terrorismus oder verbotenem Nachrichtendienst verbunden sind, fallen sie zwar wie bisher auch unter die in Ziffer 1 und 2 definierten Aufgaben. Da dieser Hintergrund aber oft – wenn überhaupt – erst nach eingehenden Abklärungen ersichtlich ist, ist es zur Sicherung der Rolle des NDB in der Cyberstrategie des Bundes notwendig, die Mitarbeit des NDB von Anfang an zu ermöglichen. Die Netzwerke der kritischen Infrastrukturen müssen gegen Angriffe von Hackern geschützt werden. Der NDB soll hier zuhanden der Stellen, die sich mit Cyberangriffen befassen, weiterhin die notwendigen Informationen über drohende oder bereits erfolgte Angriffe beschaffen und die Abwehr von Angriffen unterstützen. Er verfügt hierzu auch über exklusive internationale Kontakte.

Der Begriff «kritische Infrastrukturen» orientiert sich dabei an Definitionen aus dem Bereich des Bevölkerungsschutzes. Er ist umfassend zu verstehen und schliesst beispielsweise auch Infrastrukturen wichtiger internationaler Organisationen in der Schweiz ein.

Der Begriff «sicherheitspolitisch bedeutsame Vorgänge im Ausland» in Buchstabe b bezieht sich auf Ereignisse und Entwicklungen im Ausland die geeignet sind, die Selbstbestimmung der Schweiz und ihre demokratische und rechtsstaatliche Ordnung zu gefährden, der Schweiz schweren sicherheitspolitischen oder anderweitigen Schaden zuzufügen oder die Handlungsfähigkeit ihrer Behörden zu beeinträchtigen. Hier erbringt der NDB hauptsächlich Leistungen für das EDA in Form von analytischen Berichten und Übermittlung von Einzelinformationen.

Buchstabe c bezieht sich auf die essentielle Aufgabe des NDB, der Landesregierung zeitgerecht für die Erfüllung ihrer Aufgaben notwendige Informationen zu liefern.

Die Aufgabe, die Handlungsfähigkeit der Schweiz zu wahren, wurde deshalb ausdrücklich in den Aufgabenkatalog des NDB aufgenommen.

Ebenfalls neu aufgenommen wurde der Begriff «Wahrung wesentlicher Landesinteressen» (vgl. Erläuterungen zu Art. 3).

Die Aufzählung der Aufgaben des NDB und der damit beabsichtigten Ziele ist zu unterscheiden von den erst in den weiteren Bestimmungen des Gesetzes geregelten konkreten Befugnissen des Nachrichtendienstes.

Die Datenbeschaffung und -bearbeitung zur Beurteilung der Bedrohungslage nach *Absatz 2* ist in den Kapiteln 3 und 4 ausführlich geregelt. Alarmierungen erfolgen durch den NDB nur im Aufgabenbereich des Gesetzes. Für andere Alarmierungen bestehen andere Zuständigkeiten (z.B. bei Naturkatastrophen durch die Nationale Alarmzentrale des Bundesamtes für Bevölkerungsschutz).

Bei besonderen sicherheitsrelevanten Ereignissen (z.B. dem jährlich stattfindenden World Economic Forum oder grossen internationalen Konferenzen wie dem Frankophoniegipfel) richtet der NDB zur Erfüllung der Aufgaben nach den Absätzen 2 und 3 einen Nachrichtenverbund ein. Dieser koordiniert die Informationsbeschaffung und -verbreitung und ermöglicht den zuständigen beteiligten Stellen das ständige Verfolgen der aktuellen Lage über die Elektronische Lagedarstellung (ELD, Art. 52).

Die Information anderer Dienststellen des Bundes und der Kantone nach Absatz 3 ist in den Artikeln 58 ff. über die Weitergabe insbesondere von Personendaten präzisiert.

In *Absatz 4* wird die Funktion des NDB als federführende Behörde für nachrichtendienstliche Kontakte mit dem Ausland aufgenommen, wie sie heute in Artikel 8 BWIS festgeschrieben ist. Doppelspurigkeiten und Widersprüche im Verkehr mit ausländischen Nachrichtendiensten und Sicherheitsbehörden sollen auf diese Weise vermieden werden. Weiter präzisiert ist diese Aufgabe in Artikel 12.

Absatz 5 nimmt die präventiven Aufgaben der schon heute beim NDB angesiedelten operativen und nachrichtendienstlichen Einheit der Melde- und Analysestelle Informationssicherung MELANI auf. Diese betreibt schon heute eine Frühwarnung in einem geschlossenen Kreis von Betreibern von kritischen Infrastrukturen. Diese wichtige Funktion geht über die reine Informationsbearbeitung nach Absatz 1 Buchstabe a Ziffer 4 hinaus und wird deshalb hier ausdrücklich geregelt.

Absatz 7 hat schliesslich besondere Bedeutung für die Sicherheit des NDB, seiner Mitarbeiterinnen und Mitarbeitern und seiner Informationen. Artikel 7 enthält nähere Regelungen dazu. Parallel zum NDG erarbeitet der Bund auch eine Rechtsgrundlage für die Informations- und Objektsicherheit. Diese wird gegebenenfalls gewisse Sicherheitsbedürfnisse des NDB in allgemeiner Form für die ganze Bundesverwaltung regeln. Im Moment soll aber das NDG eigenständig sicherstellen, dass der NDB zu einem hinreichenden Schutz verpflichtet ist.

Ferner kann der NDB auch Unterstützungsleistungen im Rahmen der Amtshilfe leisten. Dies gehört indessen nicht zu seinen Hauptaufgaben und ist in Artikel 68 separat geregelt.

Art. 7 Schutz- und Sicherheitsmassnahmen

Die aufgeführten Schutz- und Sicherheitsmassnahmen ergänzen die allgemeinen Bundeserlasse zur integralen Sicherheit namentlich in den Bereichen des Personen-, Informations- und Objektschutzes. Sie dienen der Durchsetzung von Vorschriften zum Schutz der Dienstgeheimnisse und steigern dadurch die Sicherheit und Glaubwürdigkeit des NDB beim Umgang mit klassifizierten Daten.

Bei der Gewährleistung der Sicherheit haben Ausbildung und Sensibilisierungen Vorrang vor anderen Massnahmen. Aufbauend auf dieser Grundlage gehören jedoch technische Massnahmen und die Überprüfung der Einhaltung von Vorschriften zu einem wirksamen und glaubwürdigen Risikomanagement.

Buchstabe a: Taschen- und Personenkontrollen werden ausschliesslich aus Gründen der Sicherheit und unter Wahrung der Verhältnismässigkeit durchgeführt. Der NDB kann Dritte mit der Durchführung beauftragen. Die Massnahme dient dem Schutz des Eigentums des Arbeitgebers und der Einhaltung der Vorschriften zum Schutz klassifizierter Informationen. Zur Anwendung kommt sie bei den Mitarbeiterinnen und Mitarbeitern des NDB, aber auch bei temporär eingesetztem Personal wie Praktikantinnen und Praktikanten. Ebenfalls kontrolliert werden können Mitarbeiterinnen und Mitarbeiter von Unternehmen, die in den Räumlichkeiten des NDB Dienstleistungen erbringen oder handwerkliche Arbeiten ausführen. Nicht Gegenstand von Kontrollen sind Mitglieder der Aufsichtsorgane sowie Besucherinnen und Besucher. Diese werden in den Räumen des NDB ständig begleitet.

Buchstabe c: Bildüberwachungssysteme werden nicht dazu verwendet, dauerhaft das Verhalten von Personen zu überwachen. Ihr Einsatz erfolgt ausserhalb von Gebäuden bei Parkplätzen, Zu-, Ein- oder Durchgängen respektive in Räumen mit Tresoren, in Archivräumen mit klassifizierten oder besonders schützenswerten Daten sowie in Lagern mit wertvollen Gütern.

Buchstabe d: Räume, in denen Gespräche mit sehr sensiblen oder hoch klassifizierten Inhalten geführt werden, werden nach Möglichkeit so mit passiven Schutzmassnahmen (Schirmdämpfung und akustische Dämmung) ausgestattet, dass ein unerlaubter Informationsabfluss z.B. via Mobiltelefone verunmöglicht wird. Wo dies nicht möglich ist, kann der temporäre Einsatz von störenden Fernmeldeanlagen zur Unterbindung des Mobiltelefonverkehrs erfolgen. Dabei wird darauf geachtet, dass keine anderen öffentlichen Interessen oder Interessen Dritter übermässig beeinträchtigt werden. Um den Fernmeldeverkehr von Dritten nicht zu stören, erfolgt der Einsatz von Störsendern eingeschränkt auf den verwendeten Besprechungsraum und nur während der Dauer von Gesprächen, die als sensibel oder geheim klassifiziert werden. Die entsprechenden Geräte müssen den Vorschriften des Bundesamtes für Kommunikation entsprechen und zugelassen sein.

Absatz 2 ist die rechtliche Grundlage für das schon heute vom NDB betriebene separate Netzwerk für die Mehrzahl seiner Informatikanwendungen und Informationssysteme. Der NDB bearbeitet besonders viele heikle und klassifizierte Daten, weshalb der Informationssicherheit besondere Bedeutung zukommt. Der Zugriff auf das Netzwerk beschränkt sich auf Angehörige des NDB, der nachrichtendienstlichen Aufsichtsorgane sowie in sehr eingeschränktem Ausmass auf wenige Angehörige des militärischen Nachrichtendienstes, der derzeit über kein eigenes, ähnlich gesichertes Netzwerk verfügt.

Art. 8 Bewaffnung

Bei der Informationsbeschaffung in den Bereichen Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus sowie verbotener Handel mit Waffen und chemischen, biologischen und nuklearen Massenvernichtungswaffen bewegen sich die beauftragten Mitarbeiterinnen und Mitarbeiter z.B. bei der Anbahnung und Pflege von Kontakten zu menschlichen Quellen teilweise in einem gefährlichen und gewalttätigen Umfeld. Die in diesem Bereich im Inland tätigen Mitarbeiterinnen und Mitarbeiter des NDB müssen bewaffnet werden, damit sie sich selbst und menschliche Quellen oder Drittpersonen schützen können, wenn eine unmittelbare Gefahr für Leib und Leben besteht. Die Tätigkeit einer Mitarbeiterin oder eines Mitarbeiters in der Beschaffung im Inland ist in den geschilderten Fällen vergleichbar mit derjenigen einer Führerin oder eines Führers von Vertrauenspersonen (VP-Führer) im polizeilichen Bereich.

Die Waffe darf nur zur Notwehr (Art. 15 f. Strafgesetzbuch[15] [StGB]) oder in Fällen von Notstand (Art. 17 f. StGB) eingesetzt werden. Die Verhältnismässigkeit insbesondere des Schusswaffeneinsatzes ist zu wahren (Abs. 2).

Die Bestimmung entspricht weitgehend dem heutigen Artikel 5*a* BWIS. Neben den Ausführungsvorschriften des Bundesrates wird der NDB die Details für die dienstliche Bewaffnung (u.a. Vorschriften zum Nachweis der ausreichenden Ausbildung und Befähigung zum Schusswaffentragen, obligatorische Schiesstrainings) wie heute in Weisungen regeln.

Art. 9 Kantonale Vollzugsbehörden

Der Vollzug der nachrichtendienstlichen Aufgaben nach diesem Gesetzesentwurf erfolgt durch Bund und Kantone gemeinsam (vgl. Art. 81). Die kantonalen Vollzugsbehörden beschaffen auf ihrem Gebiet Informationen, die sie direkt aufgrund des NDG oder eines besonderen Auftrags des NDB beschaffen müssen. Wie bisher sollen die Kantone für diese Aufgaben eine spezialisierte Dienststelle bezeichnen. Diese befindet sich in der Regel im Polizeikorps.

Weitere Vorschriften mit Bezug zu den Kantonen befinden sich in den Kapiteln 4 (betreffend Datenbearbeitung) und 6 (betreffend Kontrolle und Aufsicht).

Art. 10 Information der Kantone

Der heutigen engen Zusammenarbeit zwischen Bund und Kantonen soll auch das neue Gesetz einen hohen Stellenwert beimessen. Es verpflichtet den Bund deshalb, wie bisher die zuständigen kantonalen Behörden über besondere Ereignisse im Aufgabengebiet des Nachrichtendienstes und über die Bedrohungslage zu informieren. Dies erfolgt vor allem über die KKPKS und die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD). Der NDB steht zudem in ständigem Kontakt mit den kantonalen Vollzugsbehörden. So ist gewährleistet, dass diese ihre Aufgaben auf kantonalem Gebiet im Einklang mit den Bedürfnissen des Bundes erfüllen können. Artikel 45 Absatz 3 regelt ergänzend dazu die Verwendung solcher Lagebeurteilungen und weiterer Daten innerhalb der Kantone.

15 SR **311.0**

Art. 11 Zusammenarbeit mit der Armee

Die Zusammenarbeit des NDB mit dem Nachrichtendienst der Armee (vor allem dem Militärischen Nachrichtendienst) und mit der Militärischen Sicherheit, wie sie seit der Gründung des NDB besteht, soll beibehalten werden.

Beide Dienste der Armee arbeiten in thematisch verwandten Bereichen der Bedrohungsbeurteilung und der Sicherheit für die Bedürfnisse der Armee. Artikel 11 regelt dabei die Pflicht des NDB, die zuständigen Stellen der Armee über armeerelevante Vorgänge zu informieren. Deren Informationspflichten sind hingegen in den Artikeln 19 und 20 (allgemeine und besondere Auskunftspflicht) geregelt. Die Details der Zusammenarbeit sollen (grundsätzlich gemäss heutigem Muster) in der Vollzugsverordnung umschrieben werden.

Absatz 2 soll es dem NDB weiterhin ermöglichen, die Verteidigungsattachés der Armee in geeigneten Fällen mit dem Beschaffen von Informationen für den NDB und der Kontaktpflege zu ausländischen Nachrichtendiensten und Sicherheitsbehörden zu beauftragen. Diese Beschaffung erfolgt dabei immer im Einklang mit der Rechtsordnung des Gaststaates, das heisst über die Nutzung der offiziellen Kontakte zu dessen Behörden oder des diplomatischen Beziehungsnetzes. Verteidigungsattachés sind somit keine «Spioninnen und Spione in Uniform», sondern bei den betroffenen Nachrichtendiensten der jeweiligen Akkreditierungsstaaten gemeldete Verbindungspersonen zum NDB. Dieses Vorgehen hat sich z.B. auch im Rahmen von Entführungsfällen oder zur Beobachtung der Entwicklungen im «arabischen Frühling» sehr gut bewährt. Die Zusammenarbeit und Aufgabenteilung erfolgt weiterhin in enger Absprache mit dem Bereich internationale Beziehungen der Armee.

Art. 12 Zusammenarbeit mit dem Ausland

Einleitend ist darauf hinzuweisen, dass der Bundesrat im NDG auf eine ausdrückliche Erwähnung des Grundsatzes verzichtet, wonach die Kantone für Sicherheitsfragen im Grenzgebiet mit den dafür zuständigen ausländischen Sicherheitsbehörden zusammenarbeiten dürfen (vgl. Art. 8 Abs. 2 BWIS). Diese Ordnung gilt ohnehin aufgrund der Bestimmung von Artikel 56 Absatz 3 der Bundesverfassung. Am bisherigen Vollzug durch die Kantone, wie er gemäss heutigem BWIS etabliert ist, ändert sich damit nichts.

Zu *Absatz 1* ist zu erwähnen, dass es im Bereich des Nachrichtendienstes derzeit keine völkerrechtlich bindenden Verträge gibt. Es werden höchstens «Agreements», allenfalls «Memorandums of Understanding» (MoU) abgeschlossen, die keine verpflichtende Wirkung haben. Der Grund dafür ist, dass der Nachrichtendienst primär den nationalen Interessen eines jeden Landes dient. Wo sich diese Interessen mit jenen von anderen Ländern decken, kann eine Zusammenarbeit stattfinden. Diese findet heute durch den NDB mit Nachrichtendiensten und Sicherheitsbehörden in zahlreichen Ländern statt, z.B. in den Bereichen der Abwehr von Terrorismus, Spionage, gewalttätigem Extremismus oder machtpolitischen und militärischen Fragen. Die Staaten wollen aber frei sein, ihre nachrichtendienstlichen Interessen ihren Bedürfnissen anpassen zu können, ohne darin durch Verträge gebunden zu sein. Die Schweiz bildet hier keine Ausnahme.

Die Weitergabe von Personendaten ins Ausland ist in Artikel 60 näher geregelt.

Eine Ausnahme könnte sich in Zukunft vor allem bezüglich des Betriebs von gemeinsamen internationalen Informationssystemen ergeben (Bst. e). Solche werden heute von den europäischen Nachrichtendiensten zunehmend gefordert, konnten jedoch nicht umfassend realisiert werden, da in den meisten Staaten die notwendigen nationalen gesetzlichen Grundlagen fehlen und auch keine internationalen Abkommen dazu bestehen. Der Bundesrat schlägt nun vor, im NDG den Grundsatz zu verankern, dass der NDB sich an automatisierten Informationssystemen beteiligen kann. Da es sich um eine besondere Form der internationalen Zusammenarbeit handelt, müsste sie aus Datenschutzgründen in einem schriftlichen technischen Abkommen geregelt werden. Für deren Abschluss im Einzelfall soll aber nicht der NDB, sondern der Bundesrat zuständig sein (Art. 69 Abs. 3).

Nach *Absatz 2* ist es künftig möglich, analog zu den Migrations-, den Verteidigungs- und den Polizeiattachés Verbindungspersonen des NDB in Schweizer Vertretungen im Ausland zu stationieren, wenn dies für die internationale Zusammenarbeit erforderlich ist. Der Einsatz erfolgt nur im Einvernehmen mit dem EDA. Die betreffenden NDB-Angehörigen sind in offizieller Mission tätig. Sie werden bei den zuständigen Stellen des Gaststaates und allfälligen Drittstaaten bei Seitenakkreditierungen ordentlich gemeldet und arbeiten ausschliesslich als offizielle Verbindungspersonen zu den zuständigen Dienststellen. Ihre Aufgabe besteht somit nicht in der verdeckten Beschaffung von nachrichtendienstlichen Informationen und sie verletzen das Recht der Gaststaaten nicht. In Anbetracht der erheblichen Kosten geht der Bundesrat davon aus, dass nur nach einem langfristigen Aufbau und nur wenige NDB-Verbindungspersonen in solche Einsätze gelangen können. Sie würden allenfalls Lücken im Dispositiv der Verteidigungsattachés schliessen bzw. dieses dort ergänzen, wo Verteidigungsattachés die benötigte Funktion nicht erfüllen können. Die finanzielle und personelle Ausstattung erfolgt hier über die ordentlichen Budgets.

Absatz 3 soll sicherstellen, dass die nachrichtendienstlichen Kontakte der Schweiz mit anderen Ländern ausschliesslich nach den Regelungen des NDG geführt werden. Der gleiche Grundsatz findet sich bereits in ähnlicher Form in Artikel 8 BWIS und ist in der geltenden Verordnung näher ausgeführt (Art. 11 Abs. 1 und 2 Verordnung vom 4. Dezember 2009[16] über den Nachrichtendienst des Bundes [V-NDB]). Die Aufgabe des NDB als «Leading-Agency» betrifft jedoch nur Kontakte mit eigentlichen Nachrichtendiensten und zu anderen ausländischen Behörden, wenn es um nachrichtendienstliche Inhalte geht. Dies betrifft vor allem den Verkehr mit ausländischen Behörden, die mehrere Funktionen ausüben (z.B. Gerichtspolizei und Inlandnachrichtendienst). Kontakte mit (kriminal-)polizeilichem Inhalt fallen in solchen Fällen in die Zuständigkeit der schweizerischen Polizeibehörden.

Der Bundesrat hat im Übr igen im Bereich der Auslandszusammenarbeit gemäss Artikel 69 des Entwurfs besondere Aufgaben und kann in diesem Zusammenhang auf dem Verordnungsweg weitere Regelungen treffen.

3. Kapitel

Nach der umfassenden Definition des Datenbearbeitungsbegriffs im DSG ist zwar die Beschaffung im Begriff der Bearbeitung enthalten (vgl. Art. 3 Bst. e DSG). Da die Beschaffung der Daten jedoch für einen Nachrichtendienst zum einen von zentraler Bedeutung ist und zum anderen aus Sicht der betroffenen Personen mit den

16 SR **121.1**

stärksten Grundrechtseingriffen verbunden sein kann, ist es gerechtfertigt, die Beschaffung und die weitere Bearbeitung in eigenständigen Kapiteln zu regeln.

Die Bestimmungen in diesem Kapitel erwähnen jeweils nur den NDB als beschaffende Stelle. Sie gelten im Rahmen ihrer Vollzugsaufträge nach den Artikeln 9 und 81 jedoch auch für die kantonalen Vollzugsbehörden.

Vereinzelt wurde in der Vernehmlassung geltend gemacht, dass die Beschaffungsmassnahmen des NDG nicht genügend auf die Strafprozessordnung[17] (StPO) abgestimmt seien. Hierzu ist festzuhalten, dass mit der Vorlage zum Nachrichtendienstgesetz nur der Bereich des Nachrichtendienstes geregelt werden soll, nicht aber jener des Strafprozesses (Einheit der Materie). Da es sich beim NDG um ein neues Gesetz handelt, muss es die aktuellen technischen Entwicklungen berücksichtigen (z.B. in Bezug auf Beschaffungsmassnahmen im Cyberraum). Weiter weist der Bundesrat darauf hin, dass der Nachrichtendienst eine eigenständige Aufgabe erfüllt und nicht eine Vorstufe oder mildere Form der Strafverfolgung darstellt. Bei den genehmigungspflichtigen Beschaffungsmassnahmen wird hingegen neu berücksichtigt, dass derzeit das BÜPF revidiert wird. Zur einfacheren Abstimmung auf diese Revision und zur Verdeutlichung, dass mit dem NDG nicht mehr oder andere Massnahmen ermöglicht werden sollen, verweist dieses nun auf das BÜPF. Dieser Verweis wird den Aufwand für die Koordination der Gesetzesvorlagen minimieren.

Nur teilweise übernommen wurde der Wunsch einzelner Kantone, über dieselben Kompetenzen wie der NDB zu verfügen. Dies trifft bei den genehmigungsfreien Beschaffungsmassnahmen teilweise zu, während die genehmigungspflichtigen gemäss NDG nur durch den Bund zu handhaben sind. Wenn ein Kanton hier eigenständige Bedürfnisse hat, so müsste er auf kantonaler Ebene legiferieren.

3. Kapitel, 1. Abschnitt

In diesem Abschnitt sind jene Beschaffungsmassnahmen aufgeführt, die der NDB selbstständig und ohne besondere externe Genehmigung einsetzen kann, weil die Eingriffsintensität relativ gering ist. Sie entsprechen weitgehend den heute in Artikel 14 Absatz 2 BWIS geregelten Beschaffungsmöglichkeiten. Das dritte Kapitel erwähnt alle klassischen nachrichtendienstlichen Beschaffungsmittel von der «open source intelligence» (OSINT, Art. 13) über die «imagery intelligence» (IMINT, Art. 14 Abs. 2) und die «human intelligence» (HUMINT, Art. 15) bis zur «communication intelligence» (COMINT, Art. 27 und 37 ff.). Für ihre Anwendung stellt das NDG je nach Intensität des Grundrechtseingriffs besondere Regeln auf.

In der Vernehmlassung war vereinzelt angeregt worden, auch den Zugriff auf Daten sozialer Netzwerke zu regeln, da solche Daten für einen Nachrichtendienst von hohem Interesse sein können. Der Bundesrat sieht jedoch von einer solchen Regelung ab, da der Begriff der «sozialen Netzwerke» wenig bestimmt ist und auf eine fast unüberschaubare Datenmenge angewendet werden könnte. Es sollen hier vielmehr die allgemeinen Regelungen zum Tragen kommen: Soweit es sich um öffentlich zugänglich gemachte Daten handelt, gelten die entsprechenden Regelungen. Für Beschaffungsmassnahmen im durch das Fernmeldegeheimnis geschützten Bereich gilt hingegen die richterliche und politische Genehmigungspflicht nach Artikel 25 ff.

17 SR **312.0**

Gemäss Artikel 81 Absatz 1 können die Kantone im selbstständigen Vollzug des NDG auf ihrem Gebiet die meisten genehmigungsfreien Beschaffungsmassnahmen ebenfalls einsetzen.

Art. 13 Öffentliche Informationsquellen

Ein Nachrichtendienst schöpft viele Informationen aus dem öffentlichen Bereich. Dies erlaubt ihm, mit besonderen nachrichtendienstlichen Mitteln noch verbleibende Lücken gezielt aufzuklären oder öffentliche Informationen mit nachrichtendienstlichen Mitteln zu bestätigen oder zu widerlegen.

Diese Beschaffungsart stellt die niedrigste Eingriffsintensität dar, da es sich um öffentliche, das heisst praktisch jedermann zugängliche Informationen handelt. Die Tatsache, dass bestimmte Informationen vor allem von Privaten nur gegen Bezahlung angeboten werden, ändert an deren öffentlichem Charakter nichts. Elektronische, gegen Entgelt zugängliche Datensammlungen sollen hier nicht anders behandelt werden als klassische Medien wie Zeitungen oder Fachpublikationen, die in der Regel auch gegen Entgelt angeboten werden.

Gegenüber dem Vernehmlassungsentwurf wurden die Informationen aus öffentlichen Registern von Behörden in diesen Artikel verschoben, weil deren Beschaffung eher einem Zugriff auf öffentliche Informationsquellen entspricht als einer Auskunftspflicht der das Register führenden Behörde.

Die Qualität öffentlich zugänglicher Informationen kann sehr unterschiedlich sein, weshalb ihre Beurteilung bei der Verwendung wichtig ist. Der Gesetzesentwurf sieht deshalb vor, die OSINT-Informationen innerhalb des NDB in einem besonderen Informationssystem verfügbar zu machen (Art. 53). Von dort aus können sie bei Bedarf beurteilt und in weitere Systeme überführt werden, wenn sie für nachrichtendienstliche Produkte verwendet werden.

Art. 14 Beobachtungen an öffentlichen und allgemein zugänglichen Orten

Absatz 1 übernimmt die bestehende Regelung von Artikel 14 Absatz 2 Buchstabe f BWIS. Das Beobachten und Festhalten von Vorgängen an öffentlichen und allgemein zugänglichen Orten gehört zu den Standardaufgaben eines Nachrichtendienstes. Treffen zwischen Führungsoffizieren ausländischer Nachrichtendienste und ihren Zuträgern finden oft an öffentlichen Orten statt, z.B. in Bahnhöfen, Flughäfen oder auf öffentlichen Plätzen. Zu den öffentlichen und allgemein zugänglichen Orten gehören auch entsprechende Bereiche von Restaurants und Hotels.

Ein Beispiel aus der Praxis: Ein in Genf unter diplomatischer Tarnung stationierter ausländischer Nachrichtendienstoffizier holte seinen Informanten öfters mit seinem Fahrzeug in der Innenstadt ab. Der Nachrichtendienstoffizier versuchte dabei den Anschein zu erwecken, er sei ein «gewöhnlicher» Diplomat.

Um solche Treffen zu dokumentieren, ist eine Beobachtung an öffentlichen und allgemein zugänglichen Orten, auch mittels Bild- und Tonaufzeichnung, unerlässlich.

Artikel 14 regelt den engeren Bereich der nachrichtendienstlichen Bildaufklärung (IMINT). Zur Erfüllung der gesetzlichen Aufgaben kann es in Einzelfällen notwendig sein, geeignete luftgestützte Mittel wie Flugzeuge, Hubschrauber oder unbemannte Einsatzmittel in der Luft, d.h. vom Boden aus gesteuerte Luftfahrzeuge,

einzusetzen. Auch weltraumgestützte Mittel wie Satelliten können geeignete Bildaufklärungsmittel darstellen (z.B. bei Entführungsfällen von Schweizer Bürgerinnen und Bürgern im Ausland). Beispielsweise lässt sich der Fortschritt von Bauten für ausländische Massenvernichtungswaffenprogramme anhand von Satellitenbildern gut beobachten. Der NDB verfügt selbst nicht über solche Mittel, kann ihren Einsatz aber bei Dritten veranlassen. Der militärische Nachrichtendienst der Schweiz verfügt über ein IMINT-Zentrum für die Beschaffung und Auswertung solcher Informationen. Satellitenbilder liefern vor allem kommerzielle Anbieter, da die Schweiz auch hier über keine eigenen Mittel verfügt.

Solche Beobachtungen sind für eine unabhängige, eigenständige Beurteilung sicherheitspolitisch relevanter Vorgänge unerlässlich. Die Beurteilungen des NDB dienen direkt der Unterstützung der Schweizer Aussenpolitik, indem z.B. Prognosen abgegeben werden können, wie viel Zeit für Verhandlungen mit einem proliferierenden Staat überhaupt noch vorhanden sein wird.

Vorgänge auf dem Boden gehören dann nicht zum öffentlichen Raum, wenn sie sich beispielsweise in einer privaten Wohnung oder auf einem privaten Grundstück abspielen. Sollten solche Vorgänge beobachtet werden, muss der NDB für die Informationsbeschaffung eine genehmigungspflichtige Massnahme nach den Artikeln 25 ff. beantragen. Wenn der private Raum nicht schon bei der Beobachtung ausgespart werden konnte (z.B. durch technische Massnahmen oder eine Begrenzung der Bildauflösung, die keine Details mehr erkennen lässt, die der Privatsphäre zuzuordnen sind), müssen die Daten vernichtet werden. Die Situation ist vergleichbar mit dem Überflug eines Passagierflugzeugs über bewohntem Gebiet: Es lässt sich auch in diesem Fall nicht verhindern, dass Passagierinnen und Passagiere durch die Fenster Vorgänge im privaten Raum auf dem Boden beobachten oder fotografieren. Jedoch wäre die Verwertung solcher Aufnahmen rechtlich anfechtbar.

Mit diesem klaren Bekenntnis zum Schutz der Privatsphäre ist nach Auffassung des Bundesrates die Gewährleistung der Grundrechte genügend sichergestellt. Gleichzeitig wird dem Nachrichtendienst nicht der Zugang zu Beobachtungsmitteln verwehrt, die sich durch den technischen Fortschritt teilweise zum Allgemeingut entwickeln.

Im Militärgesetz vom 3. Februar 1995[18] (MG) soll eine analoge Regelung für den militärischen Bereich verankert werden (Art. 99 Abs. 1quater, vgl. Änderung bisherigen Rechts).

Art. 15 Menschliche Quellen

Die Umschreibung des Begriffs «menschliche Quellen» in *Absatz 1* orientiert sich an jener nach Artikel 14*a* BWIS für Informantinnen und Informanten. Diese ist jedoch eher polizeilich orientiert. Im Sprachgebrauch des fusionierten Nachrichtendienstes ist deshalb der hier gewählte Ausdruck zutreffender.

«Menschliche Quelle» oder «human intelligence» (HUMINT) sind international anerkannte nachrichtendienstliche Ausdrücke für Personen, die exklusiven Zugang zu Informationen haben und bereit sind, dem NDB diese Informationen zu geben. Beispielsweise verwendet das belgische Gesetz vom 4. Februar 2010 über die

18 SR **510.10**

Methoden zum Sammeln von Daten durch die Nachrichten- und Sicherheitsdienste ebenfalls den Begriff «menschliche Quellen».

Es handelt sich dabei um Personen, die aus eigener Motivation, oder auf Anfrage des NDB dazu bereit sind, Informationen an den NDB weiterzugeben.

Wenn beispielsweise eine terroristische Gruppierung im In- oder Ausland Anschläge in der Schweiz oder gegen Schweizer Bürgerinnen und Bürger oder Schweizer Interessen im Ausland plant, so sind diese Informationen vielfach nur über Personen zu beschaffen, die direkten oder indirekten Zugang zu dieser Gruppierung haben. Die Planungen und Aktivitäten der Gruppierung werden oftmals aus Sicherheitsgründen nirgends schriftlich festgehalten oder ausgetauscht, sondern nur in einem begrenzten Kreis innerhalb der Gruppierung mündlich weitergegeben.

Menschliche Quellen, insbesondere Quellen im Ausland, können mitunter auch ohne ihr Wissen dem NDB Informationen liefern. Ihr Nichtwissen über ihre Abschöpfung kann ihrem eigenen Schutz dienen.

Bei den Entschädigungen nach *Absatz 2* kann es sich um die Erstattung von Auslagen handeln, die nach Absprache als Spesen entschädigt werden, oder um eine Bezahlung für Informationen, die für die Aufgabenerfüllung des NDB von grossem Nutzen sind. Insbesondere Quellen im Ausland verlangen vielfach Geld für ihre Informationen. Die Bezahlung von menschlichen Quellen kann, wenn sie offenkundig wird, sowohl im Herkunftsland als auch im persönlichen Umfeld ein grosses Risiko darstellen. Ein Verdacht auf Einkünfte aufgrund nachrichtendienstlicher Verbindungen und Tätigkeiten kann eine Quelle beruflich schädigen, ihren Ruf zerstören und sie je nach Land und Umfeld an Leib und Leben gefährden. Aus diesen Gründen dürfen Quellenentschädigungen in den meisten Fällen nach aussen weder deklariert und versteuert werden, noch dürfen sie den entsprechenden Sozialversicherungspflichten unterliegen. Ansonsten kann die Sicherheit vieler Quellen nicht gewährleistet werden, und eine Zusammenarbeit ist verunmöglicht. Nur in besonderen Fällen können die Einkünfte bisweilen über Tarnstrukturen offizialisiert werden, beispielsweise wenn eine Quelle ihren Lebensunterhalt fast ausschliesslich aus Entschädigungen des NDB bestreiten würde und deshalb keine andere hinreichende soziale Absicherung vorhanden wäre. Solche Fälle würden für die Schweiz aber absolute Ausnahmen darstellen.

Abs. 3–5: Eine menschliche Quelle kann aufgrund der Informationen über die sie verfügt und die sie an den NDB weitergibt, unter Umständen an Leib und Leben gefährdet sein. Dies trifft insbesondere auf Bereiche von terroristischen Zellen und gewalttätig- extremistischen Gruppierungen aus dem Ausland zu, aber auch auf Bereiche, in denen staatliche Organisationen und Nachrichtendienste operieren. Ausländische Quellen, die für den NDB arbeiten, können in ihren Herkunftsländern in hohem Mass gefährdet sein. Die Enttarnung könnte für die menschliche Quelle oder ihre Angehörigen in letzter Konsequenz gar das Todesurteil bedeuten:

- Atomwissenschaftlerinnen und -wissenschaftler aus asiatischen Ländern, die Informationen an ausländische Nachrichtendienste weitergeben, können in ihren Heimatländern mit dem Tod bestraft werden.
- Während der Wirren des «arabischen Frühlings» konnte der NDB aus verschiedenen Quellen feststellen, dass die in der Schweiz lebende Diaspora von Regimegegnerinnen und -gegnern wiederholt der Beobachtung oder Drangsalierung durch regierungstreue Personen aus ihrem Heimatland aus-

gesetzt war. Würde eine allfällige Zusammenarbeit von Quellen aus dem Umfeld der Regimegegnerinnen und -gegner mit dem NDB bekannt, könnte dies zu einer Gefährdung an Leib und Leben der Quellen selbst oder ihrer Angehörigen in den Heimatländern führen.

Der NDB steht gegenüber seinen menschlichen Quellen in der Pflicht, deren Unversehrtheit bestmöglich zu schützen. Bei der Quellenführung achtet er stets auf einen maximalen Quellenschutz. Zu den Massnahmen, die diesen Schutz gewährleisten, gehören in ausserordentlichen Fällen Aufenthaltsbewilligungen für eine menschliche Quelle und deren Familienangehörige in der Schweiz, aber auch eine Legendierung oder eine Tarnidentität. Während des aktiven Einsatzes einer menschlichen Quelle kann ihr eine Legende oder Tarnidentität durch den NDB nach Artikel 18 zugesprochen werden, wenn dies zu ihrem Schutz notwendig ist.

Nach Beendigung der Tätigkeit für den NDB kann die menschliche Quelle weiterhin an Leib und Leben gefährdet sein. In solchen Fällen sieht das Gesetz ebenfalls die Möglichkeit der Ausstattung mit einer Legendierung oder einer Tarnidentität vor. Dann gilt aber nicht mehr ein Überprüfungszeitraum von 12 Monaten wie im aktiven Einsatz, sondern es handelt sich eher um eine Langzeitmassnahme. Sie dauert so lange an, wie die Gefährdung der menschlichen Quelle und evtl. ihrer Angehörigen fortbesteht. Da in diesen Fällen in der Regel kein regelmässiger Kontakt des NDB zur Quelle mehr besteht, ist vorgesehen, dass die Chefin oder der Chef des VBS das Ausstatten mit einer Legendierung oder Tarnidentität genehmigen muss, damit hier auch die politischen Risiken abgewogen werden können.

Die nachrichtendienstlichen Aufsichtsorgane (vgl. Art. 74 ff.) haben Zugang zu sämtlichen Informationen bezüglich der Führung von menschlichen Quellen; sie erhalten schon nach heutiger Praxis jährlich einen ausführlichen Bericht über alle derartigen Operationen und nehmen Einblick in von ihnen ausgewählte Dossiers.

Art. 16 Personen- und Sachfahndungsausschreibungen

Mit den *Absätzen 1 und 2* soll eine ähnliche Regelung eingeführt werden, wie sie das nicht weiter verfolgte Polizeiaufgabengesetz vorgesehen hätte (3. Kapitel: Massnahmen zur Verhinderung drohender Straftaten). Der vorliegende Entwurf ist jedoch im Unterschied zum Polizeiaufgabengesetz nicht auf die Verhinderung drohender Straftaten ausgerichtet, sondern auf die Informationsbeschaffung im Hinblick auf die Abwehr von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz und die Wahrung wesentlicher Landesinteressen nach Artikel 3. Die Bedrohung der inneren oder äusseren Sicherheit bzw. ein Bundesratsbeschluss betreffend die Wahrung wesentlicher Landesinteressen (vgl. Art. 3 in Verbindung mit Art. 70) bildet deshalb die Voraussetzung für die Ausschreibung von Personen und Fahrzeugen durch den NDB (vgl. Abs. 2 Bst. a). Die Voraussetzungen von Absatz 2 gelten alternativ.

Das Gesetz verankert damit die schon heute bestehende Möglichkeit, durch die Ausschreibung von Personen und Fahrzeugen im automatisierten Polizeifahndungssystem (RIPOL) den Aufenthaltsort und die Bewegungen von bestimmten Zielpersonen (z.B. von Angehörigen terrorismusverdächtiger Gruppierungen) feststellen zu können. Die Polizeigesetzgebung verwendet hierfür den Begriff der «verdeckten Registrierung». Zusätzlich soll die Ausschreibung zukünftig auch im nationalen Teil des Schengener Informationssystems (N-SIS) erfolgen können. Wenn solche vom NDB ausgeschriebene Personen den Schengen-Raum betreten bzw. verlassen oder wenn sie innerhalb des Schengen-Raums von der Polizei oder von den Grenzkon-

trollorganen kontrolliert werden, wird die Schweiz bzw. der NDB künftig von den zuständigen ausländischen Behörden eine Mitteilung erhalten. Diese erfolgt über das Schweizer SIRENE-Büro (SIRENE für «*S*upplementary *I*nformation *RE*quest at the *N*ational *E*ntry»). Dabei handelt es sich um die Verbindungsstelle der für die SIS-Zusammenarbeit zuständigen Behörden der Schengen-Staaten (vgl. Art. 8 und 9 der N-SIS-Verordnung vom 8. März 2013[19]). Selbstverständlich ist in jedem Einzelfall abzuwägen, ob eine Ausschreibung notwendig und sinnvoll ist. Es besteht insbesondere kein Automatismus zwischen der nationalen und der Schengen-Ausschreibung.

Die in *Absatz 3* statuierte Ausnahme von der Ausschreibung im RIPOL oder im N-SIS betrifft nur die Fahrzeuge von Drittpersonen, die Berufsgeheimnissen unterstehen, und entspricht ebenfalls der heutigen Praxis. Es handelt sich dabei um diejenigen Personengruppen, die ein Zeugnisverweigerungsrecht besitzen (z.B. Geistliche, Rechtsanwälte, Träger/innen von Berufsgeheimnissen und Medienschaffende).

Die Kantone können in ihren eigenen Interessenbereichen ebenfalls solche Ausschreibungen im Rahmen der jeweiligen Polizeigesetzgebung vornehmen.

3. Kapitel, 2. Abschnitt

Der SND verfügte seit 1997 auf der Basis von Artikel 99 MG über die Möglichkeit, seine Beschaffungsorgane mit Tarnidentitäten auszustatten (vgl. Jahresbericht 2002/2003 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation vom 23. Januar 2004[20]). Seit der Zusammenlegung von DAP und SND zum NDB sieht Artikel 16 Absatz 1 Buchstabe e V-NDB in Bezug auf die Auslandbeschaffung ausdrücklich den Einsatz von Tarnpapieren und Legenden vor. Tarnidentitäten und damit verbundene Legenden werden seit 1997 durch die Mitarbeiterinnen und Mitarbeiter der Auslandbeschaffung als permanente Schutzmassnahme verwendet. Tarnidentitäten werden durch den NDB intern genehmigt, die Aufsicht hierüber üben die Chefin oder der Chef des VBS, der Sicherheitsausschuss des Bundesrates und die Geschäftsprüfungsdelegation aus.

Mit der Verabschiedung der BWIS-Revision vom 23. Dezember 2011 durch das Parlament wurde als wesentliche Neuerung mit Artikel 14*c* die Verwendung von Tarnidentitäten und dazu gehörenden Legendierungen auch für die Informationsbeschaffung im Inland ermöglicht. Im Unterschied zum NDB-internen Genehmigungsprozess für die Tarnidentitäten der Auslandbeschaffung muss die Ausstattung von Personen mit Tarnidentitäten, die mit BWIS-Aufgaben betraut sind, der Chefin oder dem Chef des VBS beantragt werden. Ausserdem wurde in Artikel 14*c* Absatz 1 Buchstabe c BWIS neu auch die Ausstattung von menschlichen Quellen des NDB mit Tarnidentitäten im Rahmen einer bestimmten Informationsbeschaffung ermöglicht.

Die Artikel 17 und 18 unterscheiden neu zwischen den Begriffen «Legendierung» und «Tarnidentität», da es sich um unterschiedliche Massnahmen handelt, die unabhängig voneinander eingesetzt werden können. Aus diesem Grund weicht die hier verwendete Terminologie auch von jener der StPO ab.

Die unterschiedlichen bisherigen Regelungen für die Genehmigung der Tarnidentitäten werden im vorliegenden Entwurf zusammengefasst und gelten sowohl für die

19 SR **362.0**
20 BBl **2004** 1673

Informationsbeschaffung im Ausland wie auch im Inland. Neu wird dem permanenten Schutzcharakter mehr Rechnung getragen. Unter Berücksichtigung der neu geschaffenen Regelung im BWIS schlägt der Bundesrat vor, die Zuständigkeit der Genehmigung von Tarnidentitäten sowohl für den Auslands- wie für den Inlandseinsatz bei der Chefin oder dem Chef des VBS anzusiedeln.

Die Genehmigung reiner Legendierungen soll aber in der Kompetenz der Direktorin oder des Direktors des NDB liegen, da hier keine falschen Ausweisdokumente hergestellt werden müssen, die falsche Namen enthalten, und auch nicht unter falschem Namen Rechtsgeschäfte getätigt werden können.

Art. 17 Legendierungen

Die Legendierung verschleiert die Angehörigkeit einer Person zum NDB. Es kann z.B. ein anderer Arbeitgeber als der NDB und eine andere berufliche Tätigkeit als die nachrichtendienstliche vorgegeben werden. Die betroffene Person behält aber ihren wahren Namen und ihre anderen biografischen Daten (Geburtsdatum, Geburtsort usw.). Eine Legendierung kann notwendig sein, um eine nachrichtendienstliche Tätigkeit überhaupt zu ermöglichen, weil beispielsweise Personen, bei denen Informationen beschafft werden sollen oder deren Umfeld nichts mit dem NDB zu tun haben wollen oder weil ein offensichtlicher Bezug der beschaffenden Person zum NDB eine Gefährdung mit sich bringen würde (weil dies z.B. in einem entsprechenden Staat als Spionage gewertet und streng geahndet würde).

Es ist nicht möglich, als Mitarbeiterin oder Mitarbeiter des NDB für eine verdeckte Beschaffungsaktion ins Ausland zu reisen und dabei als nachrichtendienstliche Mitarbeiterin oder als nachrichtendienstlicher Mitarbeiter identifizierbar zu sein. Ansonsten könnten die betreffenden Mitarbeiterinnen und Mitarbeiter und die Quellen, mit denen sie in Kontakt stehen, möglicherweise enttarnt und damit gefährdet werden. Auch in der Schweiz können Mitarbeiterinnen und Mitarbeiter des NDB und ihre Quellen insbesondere im Umfeld des Terrorismus oder des verbotenen Nachrichtendienstes gefährdet werden, wenn ein Bezug zum NDB erkennbar ist.

Aufgrund der Entwicklung der Biometrie ist es in zunehmendem Masse nicht mehr möglich, mit anderen Identitäten als der eigenen ins Ausland zu reisen. Um die nachrichtendienstlichen Tätigkeiten im Ausland weiterhin zu gewährleisten, ist es daher notwendig, die Möglichkeit für eine Legendierung der wahren Identität zu schaffen.

Der Aufbau von Legenden ist oft eine langfristige Massnahme und nicht an einzelne Operationen gebunden. Je nach Schutzbedürfnis kann dafür eine kurze (z.B. Beschaffen von Prepaid-Telefon und Herstellen fiktiver Visitenkarte) oder eine längere (z.B. Finden/Kreieren eines fiktiven Arbeitgebers, Sicherstellung einer überprüfbaren Erreichbarkeit mit Telefon, E-Mail usw.) Zeitspanne benötigt werden. Als Urkunden gelten dabei Schriften oder ihnen gleichgestellte Bild- und Datenträger, die bestimmt oder geeignet sind, eine Tatsache von rechtlicher Bedeutung zu beweisen (vgl. Art. 110 Abs. 4 StGB). Die Verwendung von Legenden entspricht der bisherigen Praxis der Auslandbeschaffung, die auf Artikel 16 Absatz 1 Buchstabe e V-NDB gründet. Diese Praxis soll mit dem vorliegenden Artikel auf eine klare rechtliche Basis gestellt werden. Soweit zur Herstellung der Legenden die Unterstützung von Schweizer Behörden notwendig ist, sollen diese zur Zusammenarbeit verpflichtet sein. Dies kann z.B. der Fall sein, wenn für die Glaubhaftigkeit der Legende

bestimmte amtliche Urkunden benötigt werden (z.B. für das Glaubhaftmachen einer bestimmten Geschäftstätigkeit).

Auf Wunsch der Kantone in der Vernehmlassung stellt der neue *Absatz 2* klar, dass der NDB keine Mitarbeiterinnen und Mitarbeiter kantonaler Sicherheitsbehörden ohne Absprache mit den kantonalen vorgesetzten Stellen mit Legenden ausstattet.

Keine Verwendung von Urkunden liegt vor, wenn die Zugehörigkeit zum NDB nur verschwiegen oder mit generellen, aber wahrheitsgetreuen Angaben verschleiert wird (z.B. Bundesangestellter, Mitarbeiterin VBS, Jurist). *Absatz 5* stellt klar, dass hierzu keine Bewilligung der Direktorin oder des Direktors erforderlich ist.

Mit der Verpflichtung zur jährlichen Berichterstattung an die Departementsleitung ist die kontinuierliche Aufsicht gewährleistet.

Art. 18 Tarnidentitäten

Eine Tarnidentität gibt einer Person eine andere Identität, das heisst einen anderen Namen und allenfalls andere biografische Daten (Geburtsdatum, Geburtsort usw.). Sie unterliegt deshalb wesentlich strengeren Voraussetzungen als die blosse Legendierung. Tarnidentitäten können wie die Legendierung auch die Verschleierung des Bezugs zum NDB bzw. das Vorgeben eines anderen Arbeitgebers als des NDB enthalten. Wenn es hingegen lediglich um den Schutz der Mitarbeiterin oder des Mitarbeiters als Person geht und nicht um dessen Tätigkeit für den NDB, so kann auch eine Tarnidentität ohne abweichende Legende erstellt werden.

Nachrichtendienste sind zur Wahrnehmung ihrer Aufgaben und insbesondere zum Schutz ihrer Mitarbeiterinnen und Mitarbeiter der Informationsbeschaffung im Ausland und in bestimmten Umfeldern im Inland auf die Verwendung von Tarnidentitäten und die zugehörigen Legenden angewiesen. Rückschlüsse auf die wahre Identität der Mitarbeiterinnen und Mitarbeiter der Beschaffung, z.B. im Umfeld des Terrorismus oder des verbotenen Nachrichtendienstes, können die Mitarbeiterinnen und Mitarbeiter und auch ihre Familienangehörigen Druckversuchen, Drohungen und auch konkreten physischen Bedrohungen aussetzen. Tarnidentitäten sind daher in erster Linie eine permanente Schutzmassnahme für die Mitarbeiterinnen und Mitarbeiter, die mit der Beschaffung von Informationen beauftragt sind.

Neben der Schutzaufgabe können Tarnidentitäten fallweise notwendig sein, um überhaupt die Anbahnung und Pflege von Kontakten zu Personen und Strukturen zwecks Informationsbeschaffung zu ermöglichen. Im Umfeld des Terrorismus oder des verbotenen Nachrichtendienstes oder einer Beschaffung im Ausland kann jeglicher Bezug einer Mitarbeiterin oder eines Mitarbeiters zum NDB einen Versuch zur Beschaffung von Informationen von vornherein verunmöglichen.

Die Schaffung solcher Tarnidentitäten ist oft auf Dauer angelegt und kann selten erst mit der Aufnahme eines bestimmten Falls begonnen werden. Je nach Intensität der Tarnung können mehrjährige Vorbereitungs- und Aufbauarbeiten bis zur Fertigstellung der erforderlichen glaubwürdigen Tarnung notwendig sein.

Absatz 1 schafft die Grundlage für die Ausstattung von Personen mit Tarnidentitäten zur Gewährleistung ihrer Sicherheit und zum Zweck der Informationsbeschaffung. Der Personenkreis, der mit Tarnidentitäten ausgestattet werden kann, wird in Absatz 1 abschliessend aufgezählt.

Da der Aufbau von Tarnidentitäten längere Zeit beansprucht und eine permanente Schutzmassnahme darstellt, ist die Ausstattung der mit der nachrichtendienstlichen Informationsbeschaffung betrauten Mitarbeiterinnen und Mitarbeitern eine grundlegende Aufgabe des Dienstes, die wegen der Verwendung von falschen Identitätsdokumenten von der Chefin oder dem Chef des VBS genehmigt werden muss. Durch die Genehmigung auf Departementsstufe ist die Aufsicht gewährleistet. Die Geschäftsprüfungsdelegation hat auch hier Zugang zu sämtlichen Informationen und Dossiers, die sie verlangt (vgl. Art. 77).

Die Verwendung der Tarnidentitäten ist befristet und kann bei Bedarf verlängert werden (vgl. Abs. 2). Sie unterliegt genauen Kriterien, die gemäss Absatz 3 in jedem Fall eingehalten werden müssen.

Mit der Schaffung einer Tarnidentität ist auch das Recht verbunden, unter ihr Rechtsgeschäfte zu tätigen, namentlich Tarnstrukturen zu errichten, die den Bezug zum NDB verbergen. Im Gegensatz zum Aufbau von Legenden zur wahren Identität (Art. 17) sind die Anforderungen an Legenden zu Tarnidentitäten und deren Aufbau oftmals aufwendiger, da sie eine andere (fiktive) Identität mit (plausiblem) Arbeitgeber, Wohnadresse usw. verbinden und glaubhaft machen müssen. 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 anderen juristischen Personen als Grundlage für eine Tarnidentität und die dazugehörende Legende).

Nach *Absatz 2* ist die Verwendung von Tarnidentitäten befristet und muss nach einem gewissen Zeitraum überprüft werden. Damit kann sichergestellt werden, dass Tarnidentitäten nur solange verwendet werden, als sie zum Schutz der Mitarbeiterinnen und Mitarbeitern und ihrer Quellen notwendig sind. Eine absolute Befristung ist indessen nicht sinnvoll. So muss z.B. ein Führungsoffizier seinen Quellen gegenüber immer mit derselben Identität auftreten. Deshalb kann diese nicht nach einer Höchstdauer verfallen, sondern muss sich nach den dienstlichen Bedürfnissen richten.

Um die notwendige Flexibilität zu wahren und um die mit der Verwendung von Tarnidentitäten durch Quellen einhergehenden Risiken besser kontrollieren zu können, wird die Verwendung von Tarnidentitäten durch menschliche Quellen auf 12 Monate befristet.

Absatz 3 legt Kriterien für die Benutzung von Tarnidentitäten zur Informationsbeschaffung fest, indem er auf das Verhältnismässigkeits- und das Subsidiaritätsprinzip verweist.

Absatz 4 ermöglicht die Herstellung der Ausweispapiere und weiterer Unterlagen: Der NDB ist dabei auf die Mitarbeit der dafür zuständigen Behörden angewiesen, die zur Zusammenarbeit verpflichtet sind. Der Hauptzweck einer Tarnidentität ist der Schutz von besonders gefährdeten Personen, indem diesen für die Zeit der besonderen Gefährdung eine andere Identität verliehen wird. Ausländischen Personen sollen dabei schweizerische Identitätspapiere nur ausnahmsweise und äusserst zurückhaltend zur Verfügung gestellt werden. Das vorübergehende Ausstellen von Schweizer Papieren gewährt in diesen Fällen selbstverständlich keine dauerhafte schweizerische Staatsangehörigkeit.

Art. 19 Auskunftspflicht bei einer konkreten Bedrohung

Der NDB ist aufgrund seiner Aufgabenstellung auf Informationen angewiesen, die ihm andere Behörden (Behörden von Bund und Kantonen, Organisationen mit öffentlichen Aufgaben) geben können. Solche Mitteilungen können auf Anfrage des NDB oder, wenn die andere Stelle eine mögliche Sicherheitsgefährdung identifiziert, unaufgefordert erteilt werden.

Bei schwerwiegenden Bedrohungen der inneren oder äusseren Sicherheit gehen die Interessen der staatlichen Gemeinschaft an der Erteilung der Auskunft dem Anspruch der betroffenen Bürgerinnen und Bürger an der Wahrung der Privatsphäre grundsätzlich vor. Leitgedanke ist, dass sich die Gemeinwesen (Bund, Kantone, Gemeinden) solidarisch an der Abwehr beteiligen sollen, wenn eine konkrete Bedrohung für die Sicherheit der Schweiz und ihrer Bürgerinnen und Bürger vorliegt.

Die Absätze 1 und 2 legen für bestimmte Bedrohungen Auskunftspflichten fest, sofern diese Bedrohungen geeignet sind, bedeutsame Rechtsgüter zu verletzen. Die einzelnen Bedrohungsquellen sind in Absatz 2 abschliessend aufgezählt. Es geht dabei um terroristische Tätigkeiten, verbotenen politischen, wirtschaftlichen oder militärischen Nachrichtendienst, um Proliferation, um Angriffe auf kritische Infrastrukturen sowie um gewalttätigen Extremismus. Die Bestimmung verpflichtet nach den Grundsätzen der Amtshilfe grundsätzlich alle Behörden und Verwaltungseinheiten des Bundes und der Kantone zur Auskunft. Die Begründung gegenüber den angefragten Stellen muss dabei wie im heute geltenden Recht nicht besonders detailliert sein oder gar Beweischarakter haben. Die angefragte Stelle muss wissen, in Bezug auf welches Arbeitsgebiet des NDB die Auskunft eingeholt wird.

Absatz 2 konkretisiert in gewisser Weise die in Artikel 6 aufgeführten Aufgabengebiete des NDB, jedoch nicht im Sinne von Legaldefinitionen von Begriffen wie «Terrorismus», sondern durch eine Beschreibung der Bedrohungen, wie dies bisher in Artikel 13*a* BWIS erfolgt.

Soweit die Auskunftspflicht durch die Wahrung wesentlicher Landesinteressen nach Artikel 3 begründet wird, bedarf sie eines entsprechenden Beschlusses des Bundesrates (vgl. dazu auch Erläuterungen zu Art. 3 und 70).

Der Artikel entspricht weitgehend dem mit BWIS II neu eingeführten Artikel 13*a* BWIS. Die entsprechenden Formulierungen sind in der sicherheitspolitischen Praxis des Nachrichtendienstes eingeführt, weshalb auch nicht auf andere Umschreibungen wie zum Beispiel die strafrechtlich orientierte zur Finanzierung des Terrorismus von Artikel 260^{quinquies} StGB zurückgegriffen wurde.

Nicht mehr separat als auskunftspflichtig aufgeführt sind die im BWIS noch besonders erwähnten Steuerbehörden. Diese unterstehen ebenfalls der Auskunftspflicht, da sie zu den in Absatz 1 genannten Behörden gehören. Eine besondere Erwähnung würde zudem fälschlicherweise den Eindruck erwecken, dass Steuerbehörden dem NDB besonders oft Informationen liefern würden. Dies trifft indessen nicht zu. Aufgrund von Unsicherheiten, die während der Vernehmlassung zu Tage traten, sei zudem bestätigt, dass Kantonalbanken in Bezug auf diese Bestimmung nicht als Dienststellen der Kantone betrachtet werden können. Das Bankkundengeheimnis wird somit auch von Kantonalbanken gegenüber dem Nachrichtendienst weiterhin gewahrt.

Zu den auskunftspflichtigen Behörden der Kantone gehören auch diejenigen der Gemeinden; sie sind vom Begriff «Kanton» miterfasst.

Organisationen, die öffentliche Aufgaben wahrnehmen, werden ebenfalls zur Auskunft verpflichtet. Es handelt sich dabei um mit Verwaltungsaufgaben betraute Organisationen und Personen des öffentlichen oder privaten Rechts nach Artikel 2 Absatz 4 RVOG, die nicht der Bundesverwaltung angehören.

Der Begriff «im Einzelfall» soll verdeutlichen, dass die verpflichteten Behörden und Organisationen zwar dauerhaft, aber nur bezogen auf bestimmte konkrete Einzelfälle und erst auf Ersuchen des NDB (oder der in seinem Auftrag handelnden kantonalen Vollzugsbehörden) Auskunft zu erteilen haben. Weil die Auskunftspflicht nur einzelfallweise und bezogen auf konkrete Bedrohungen gegeben ist, rechtfertigt sich der relativ breit gefasste Adressatenkreis.

Gemäss Artikel 81 Absatz 1 können die kantonalen Sicherheitsorgane unter Anrufung dieses Artikels auch selbstständig Informationen zum Vollzug des NDG beschaffen. Bei einer Weiterleitung der Erkenntnisse an den Bund werden die dabei beschafften Daten zu Bundesdaten.

Absatz 4 regelt den Fall, dass eine dritte Behörde selbstständig eine Bedrohung der inneren oder äusseren Sicherheit feststellt. Sie soll dann die Möglichkeit haben, den Sachverhalt dem NDB zur Kenntnis zu bringen. Das Gegenstück zu dieser Bestimmung bei Vorliegen eines strafrechtlich relevanten Tatverdachtes ist Artikel 22*a* des Bundespersonalgesetzes vom 24. März 2000[21], der Angestellte von Bundesbehörden verpflichtet, jeden Verdacht auf eine von Amtes wegen zu verfolgende strafbare Handlung zur Anzeige zu bringen.

Art. 20 Besondere Auskunfts- und Meldepflicht

Absatz 1 nennt die dem Vollzug von Sicherheitsaufgaben besonders nahestehenden Behörden und Amtsstellen, die zur Erstattung von Auskünften verpflichtet sind. Die Auskunftspflicht geht dabei weiter als diejenige nach Artikel 19 (Allgemeine Auskunftspflicht): Sie ist weder auf einzelne Themenbereiche beschränkt noch an besondere Voraussetzungen gebunden und dient dem Vollzug des Gesetzes als solchem. Sie ist dafür anders als in Artikel 19 auf den genannten Kreis von Amtsstellen beschränkt. Eine Ausdehnung auf Sozial- und Steuerbehörden, wie in der Vernehmlassung teilweise vorgeschlagen, hält der Bundesrat für unnötig und unverhältnismässig.

Gemeint ist mit der Bestimmung nach Absatz 1 nicht eine integrale Auskunftspflicht, sondern eine Auskunftspflicht, die sich auf konkrete Fälle und Organisationen bezieht.

Die Auskunftspflichten beziehen sich jeweils auf die spezifischen Aufgaben der genannten Behörden. Namentlich mit Bezug auf Buchstabe i bedeutet dies, dass für den Betrieb von Informatiksystemen zuständige Behörden nur zu Auskünften bezüglich des technischen Betriebs der Systeme verpflichtet sind, aber nicht über Inhalte, z.B. über Inhalte der betriebenen Datenbanken. Dieser Buchstabe zielt denn auch auf den Bereich der Cybersicherheit und den Schutz kritischer Infrastrukturen.

Absatz 3 regelt wiederum den Fall, dass eine dritte Behörde selbstständig eine Bedrohung der inneren oder äusseren Sicherheit feststellt.

21 SR **172.220.1**

Absatz 4 entspricht dem geltenden Recht von Artikel 11 Absatz 2 Buchstabe a BWIS. Ein grösserer Teil der Meldepflichten ist in Anhang 1 V-NDB publiziert. Meldepflichten zu Vorgängen und Feststellungen, die aus Geheimhaltungsgründen nicht veröffentlicht werden dürfen, sollen wie bisher in einer vertraulichen Liste festgehalten werden. Die betroffenen Amtsstellen werden über ihre Meldepflichten einzeln informiert, und die Geschäftsprüfungsdelegation hat Zugang zu sämtlichen für die Aufsicht benötigten Informationen.

Art. 21 Verfahren bei Meinungsverschiedenheiten über Auskunfts- und Meldepflichten

Absatz 1 regelt das Verfahren für den Fall, dass innerhalb der Bundesverwaltung Meinungsverschiedenheiten auftreten. Entscheidinstanz ist bei Meinungsverschiedenheiten innerhalb des VBS die Chefin oder der Chef des VBS, bei solchen mit Ämtern anderer Departemente der Bundesrat als jeweils gemeinsame Aufsichtsbehörde. Dies entspricht der allgemeinen Regelung der Verwaltungsorganisation.

Absatz 2 regelt das Verfahren für den Fall, dass zwischen Bund und Kantonen Meinungsverschiedenheiten auftreten. In einem solchen Fall ist das Bundesverwaltungsgericht zuständig.

Art. 22 Meldungen und Auskünfte von Dritten

Das Einholen von Auskünften durch den NDB oder die kantonalen Vollzugsbehörden erfolgt auf freiwilliger Basis bei den betroffenen Privatpersonen. Bei der bewilligten Verwendung von Legenden, welche die Zugehörigkeit zu nachrichtendienstlichen Dienststellen verschleiern, kann die befragte Person allerdings nicht auf diese Freiwilligkeit aufmerksam gemacht werden, weil sonst die Legende aufgedeckt werden müsste. Untersteht eine meldende oder auskunftserteilende Person einem Berufsgeheimnis oder anderen gesetzlichen Geheimhaltungsvorschriften, muss sie diese – wie gegenüber jeder anderen Person oder Amtsstelle – auch gegenüber dem NDB bzw. den kantonalen Vollzugsbehörden beachten.

Absatz 3 kommt nur bei Legendierungen zum Tragen, weil Tarnidentitäten vor allem bei der Beschaffung im Inland nicht zwangsläufig mit einer Verschleierung der Zugehörigkeit zum NDB verbunden sein müssen.

Art. 23 Identifikation und Befragung von Personen

Dieser Artikel wurde erst nach der Vernehmlassung eingeführt, um eine gewisse Diskrepanz zum heutigen BWIS zu beseitigen, welches dem NDB das Nachforschen nach der Identität und dem Aufenthalt von Personen erlaubt. Die neue Regelung wurde in Anlehnung an Artikel 215 StPO formuliert, der die polizeiliche Anhaltung im Interesse der Aufklärung einer Straftat regelt. Kantonale Polizeigesetze enthalten in der Regel vergleichbare Bestimmungen zur Erfüllung reiner Sicherheitsaufgaben.

Die Anhaltung und Identifikation dient im hier geregelten Fall jedoch der nachrichtendienstlichen Aufgabenerfüllung mit Bezug auf die klassischen Aufgabenbereiche im Inland: Abwehr von Terrorismus, Spionage, gewalttätiger Extremismus, Proliferation und Angriffe auf kritische Infrastrukturen. Die Anhaltung und die Befragung dürfen nur so lange dauern, wie es der Zweck erfordert.

Die Festlegung einer Höchstdauer ist wie in der Strafprozessordnung nicht sinnvoll, weil die Dauer stark von den konkreten Umständen abhängt und in Bezug auf diese verhältnismässig sein muss. So darf eine reine Personenkontrolle lediglich ein paar Minuten dauern, während eine Befragung unter Umständen bis zu wenigen Stunden dauern kann, wenn dazu beispielsweise ein geschützter Ort aufgesucht wird. Die Gesamtdauer muss in Analogie zur Abgrenzung zwischen der polizeilichen Anhaltung und der polizeilichen Festnahme gemäss StPO (Art. 215 ff.) unter drei Stunden liegen.

Die Befragung findet nach Artikel 22 statt. Der befragten Person steht es somit frei, ob sie die Fragen beantworten will oder nicht.

Art. 24 Besondere Auskunftspflichten Privater

Absatz 1 übernimmt die 2012 mit Artikel 13*c* in das BWIS aufgenommene Verpflichtung zur Auskunftserteilung für gewerbliche Transporteure und erweitert diese um Auskünfte von privaten Betreiberinnen und Betreibern von Sicherheitsinfrastrukturen wie Videoüberwachungsanlagen. Auch elektronische Zutrittssysteme können vergleichbare, wichtige Informationen liefern. Wie schon unter dem BWIS ist dadurch niemand verpflichtet, bestimmte Daten zu erheben oder aufzubewahren. Die Bestimmung soll lediglich gewährleisten, dass Zugang zu den ohnehin vorhandenen Daten gewährt wird, wenn eine konkrete Bedrohung besteht.

Solche Auskünfte könnten z.B. wichtig sein, um Reisebewegungen von Zielpersonen festzustellen, die in Terrorismus, gewalttätigen Extremismus, verbotenen Nachrichtendienst und Proliferation involviert sind. Adressaten können beispielsweise Fluggesellschaften, Reiseunternehmen und Mietwagenfirmen sein. Bei den privaten Betreibern von Sicherheitsinfrastrukturen wird es in der Regel um Unternehmen gehen, die eigene oder fremde Infrastrukturen schützen, zum Beispiel aus den Bereichen Verkehr, Transport, Energie oder Verkauf.

Absatz 2 verweist auf die schon heute gemäss BÜPF bestehende Möglichkeit, über den Dienst «Überwachung Post- und Fernmeldeverkehr» (Dienst ÜPF) im EJPD Informationen über Fernmeldeanschlüsse einer Person und andere ihr zugeteilte Adressierungselemente einzuholen bzw. darüber, welcher Person bestimmte Adressierungselemente (z.B. Telefonnummern) zugewiesen sind. Entsprechend wird auch Artikel 14 Absatz 2bis BÜPF angepasst.[22] Es handelt sich dabei um Auskünfte, die nicht dem Fernmeldegeheimnis unterstellt sind.

Die Durchsetzung der Auskunftspflicht Privater erfolgt im Bedarfsfall auf dem Weg des Bundesverwaltungsverfahrens durch Erlass einer beschwerdefähigen Verfügung, wenn nötig unter Verweis auf Artikel 292 StGB (Ungehorsam gegen eine amtliche Verfügung). Eine vorgängige richterliche Genehmigung des Auskunftsersuchens erscheint daher unverhältnismässig.

Verfügungen des NDB können nach Artikel 79 mit Beschwerde angefochten werden. Die Beschaffung von Informationen, z.B. über Personen, die terroristischer Tätigkeiten zum Nachteil der Schweiz verdächtigt werden, geschieht oft unter Zeitdruck. Wenn erst der Ausgang eines Beschwerdeverfahrens abgewartet werden müsste, könnte sich z.B. die nachträglich gelieferte Information eines Transportun-

22 Im Entwurf zum totalrevidierten BÜPF (BBl **2013** 2789; Botschaft: BBl **2013** 2683) findet sich die entsprechende Bestimmung in Art. 15.

ternehmens als nutzlos erweisen. Deshalb sieht die Vorlage vor, dass eine Beschwerde keine aufschiebende Wirkung hat (Art. 79 Abs. 3).

3. Kapitel, 4. Abschnitt

Für die Wahrnehmung seiner Aufgaben, insbesondere für das frühzeitige Erkennen und Einschätzen von Bedrohungen und Gefahren, die die Entscheidungs- und Handlungsfähigkeit der Schweizer Behörden einschränken oder die demokratischen Grundlagen und staatlichen Strukturen gefährden, ist der NDB auf wirksame Mittel zur Beschaffung von Informationen angewiesen.

Die nachrichtendienstlichen Organe von Bund und Kantonen sehen sich vor allem im Bereich des Terrorismus mit immer brutaleren und rücksichtsloseren Gegnern konfrontiert:

Zwischen dem 11. und 19. März 2012 wurden in den südfranzösischen Städten Toulouse und Montauban sieben Menschen auf offener Strasse erschossen, darunter auch Kinder. Beim Täter handelte es sich um einen Franzosen algerischer Herkunft, der über sich selbst sagte, dass er der Terrorgruppierung Al-Qaïda angehöre. Es war den französischen Behörden bekannt, dass er Reisen nach Afghanistan und Pakistan unternommen hatte. Er pflegte Kontakte zu einer radikalen Salafisten-Bewegung in Frankreich.

Dem NDB sind mehrere Personen mit Bezügen zur Schweiz bekannt, bei denen Parallelen zur Radikalisierung, wie sie im Fall von Toulouse und Montauban beschrieben wurden, vorliegen. Solche Personen haben sich über das Internet radikalisiert und sich in terroristischen Ausbildungslagern im Ausland aufgehalten. Radikalisierte Einzeltäter wie in den Fällen von Toulouse und Montauban führen ein nach aussen hin unauffälliges Leben und machen den Anschein, gut in die Gesellschaft integriert zu sein. Ihre wahren Absichten teilen sie oft nicht einmal ihrem engsten Umfeld mit. So erhalten die Behörden kaum Hinweise aus der Bevölkerung. Um frühzeitig Erkenntnisse über diese Personen beschaffen zu können, sind die Behörden immer mehr auf den Einsatz besonderer Beschaffungsmassnahmen angewiesen, wie sie in diesem Gesetzesentwurf vorgeschlagen werden. Auch wenn die Schweiz zurzeit nicht Zielscheibe des internationalen Terrorismus ist, so vermag niemand vorauszusagen, ob dies in Zukunft nicht doch der Fall sein wird.

Auch in den anderen Aufgabengebieten des NDB arbeitet die Gegenseite oft konspirativ, sei dies im verbotenen Nachrichtendienst, in der Proliferation oder in Angriffen auf kritische Infrastrukturen. Mit Informationsbeschaffungen im vorwiegend öffentlichen Raum sind hier Erkenntnisse über Tätigkeiten und Absichten nur sehr schwer zu erzielen.

Mit den heutigen Beschaffungsmitteln, die im Wesentlichen auf der Beschaffung aus öffentlichen Quellen, dem Einholen von Auskünften und dem Beobachten an öffentlichen Orten basieren (Art. 14 BWIS), kann der NDB nach Einschätzung des Bundesrates seine Aufgabe nur mehr bedingt erfüllen. Viele Vorgänge zur Beurteilung von Bedrohungen finden nicht im öffentlichen Raum statt. Eine konspirative Kommunikation kann im allgemein zugänglichen Internet kaum festgestellt werden. Soll der NDB seine Rolle als präventives Sicherheitsorgan des Bundes effizient wahrnehmen und die Erwartungen an seine gesetzlichen Aufgaben erfüllen, muss er die Möglichkeit haben, in besonderen Fällen zusätzliche wirksame Beschaffungsmassnahmen einzusetzen.

Der Bundesrat schätzt, dass bei der heutigen Bedrohungslage in rund zehn Fällen pro Jahr genehmigungspflichtige Beschaffungsmassnahmen in Frage kommen, wobei pro Fall mehrere Massnahmen denkbar sind (z.B. Überwachung mehrerer Fernmeldeanschlüsse sowie Ortung eines Fahrzeuges und Durchsuchen eines Hotelzimmers derselben Person). Es handelt sich dabei um Fälle mit einem besonders grossen Bedrohungspotenzial in den Bereichen Terrorismus, verbotener Nachrichtendienst, Proliferation und Angriffe auf kritische Infrastrukturen oder Wahrung wesentlicher Landesinteressen nach Artikel 3; in diesen Fällen würden die anderen Beschaffungsmassnahmen nicht ausreichen, um für die Wahrung der Sicherheit der Schweiz elementare Informationen zu erhalten.

Die genehmigungspflichtigen Beschaffungsmassnahmen umfassen insbesondere (Art. 25):

- die Überwachung des Post- und Fernmeldeverkehrs nach dem BÜPF[23];
- das Orten des Standorts von Personen oder Sachen durch die Lokalisierung eines von der Person verwendeten Mobiltelefongeräts (nach dem BÜPF) oder durch besondere Ortungsgeräte (in der Regel GPS-Empfänger mit oder ohne Sendeeinrichtung);
- den Einsatz von Überwachungsgeräten zum Abhören von Gesprächen und zur Beobachtung von Vorgängen in privaten Räumen;
- das Eindringen in Computersysteme und Computernetzwerke, um dort vorhandene oder übermittelte Informationen zu beschaffen, oder den Zugriff auf Informationen zu stören, zu verhindern, oder zu verlangsamen, wenn von diesen Systemen Angriffe gegen kritische Infrastrukturen ausgeführt werden;
- das Durchsuchen von Räumlichkeiten, Fahrzeugen oder von Personen mitgeführten Behältnissen, um dort vorhandene oder übermittelte Informationen oder Gegenstände zu beschaffen. Die Durchsuchung kann verdeckt und ohne Kenntnis der an den Räumlichkeiten, Fahrzeugen oder Behältnissen Berechtigten durchgeführt werden.

Diese Massnahmen müssen durch das Bundesverwaltungsgericht bewilligt und durch den Chef oder die Chefin des VBS nach vorgängiger Konsultation des Sicherheitsausschusses freigegeben werden, bevor der NDB sie einsetzen kann. Wenn Gefahr im Verzug ist, kann die Direktorin oder der Direktor des NDB ausnahmsweise den sofortigen Einsatz einer Massnahme anordnen. Der Antrag an das Bundesverwaltungsgericht muss sodann innerhalb von 24 Stunden erfolgen (Art. 30 Abs. 2).

Es ist zu betonen, dass diese Informationsbeschaffungen nur Fälle von sicherheitspolitisch relevanten Bedrohungen betreffen, in welchen keine strafrechtlichen Ermittlungen erfolgen. Ist die Bedrohung mit dem Verdacht einer strafbaren Handlung verbunden, so sind die Strafverfolgungsbehörden zu informieren (vgl. Art. 59). Ein allfälliges Strafverfahren und in dessen Rahmen verfügte Überwachungsmassnahmen gehen den Informationsbeschaffungen nach diesem Gesetz vor. Jedoch sind nicht alle sicherheitspolitisch relevanten Bedrohungen strafrechtlich relevant bzw.

23 Derzeit ist eine Totalrevision des BÜPF in parlamentarischer Beratung, siehe auch Ausführungen unter Ziffer 14 der Änderungen bestehender Erlasse.

genügen die Verdachtslagen teilweise noch nicht, um strafrechtliche Ermittlungen auszulösen.

Das Gesetz soll diese einschneidenden Massnahmen nur in wichtigen Fällen, in denen die Sicherheit der Schweiz bedroht ist, erlauben. Hierfür definiert es strenge Voraussetzungen und ein mehrstufiges Genehmigungsverfahren.

Wie zu allen Vollzugsbereichen des NDG hat die Geschäftsprüfungsdelegation vollen Zugang zu allen für die Aufsicht benötigten Daten und Akten.

Art. 25 Arten von genehmigungspflichtigen Beschaffungsmassnahmen

Absatz 1 Buchstabe a ermöglicht es dem NDB, die Überwachung des Post- und Fernmeldeverkehrs gemäss den Bestimmungen des BÜPF anzuordnen. Im Gegensatz zu den Strafverfolgungsbehörden, die solche Überwachungen im Rahmen eines Strafverfahrens zur Überführung eines Täters einsetzen (repressive Zielsetzung), wird der NDB die Post- und Fernmeldeüberwachung ausschliesslich zu präventiven Zwecken anordnen. Ziel ist das frühzeitige Erkennen von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz. Wenn der NDB im Rahmen seiner Abklärungen den Verdacht hat, dass strafbare Handlungen vorliegen, wird er die Strafverfolgungsbehörden informieren.

Im Gegensatz zum Vorentwurf, der zur besseren Verständlichkeit in der Vernehmlassung die Überwachungsmassnahmen im Bereich des Post- und Fernmeldeverkehrs einzeln aufgezählt hatte, verweist der Gesetzestext neu generell auf die Überwachungsarten nach dem BÜPF. Damit wird die Koordination mit dem in Totalrevision befindlichen BÜPF[24] erleichtert, und es werden in der Vernehmlassung aufgetretene Missverständnisse – dass mit dem NDG andere Überwachungsarten und neue Verpflichtungen für die Anbieterinnen von Fernmeldediensten (nachfolgend Anbieterinnen) eingeführt würden – vermieden. Die Abwicklung der Überwachungen erfolgt denn auch über den Dienst ÜPF.

In der Vernehmlassung machten verschiedene Anbieterinnen geltend, dass die Entschädigungen für die Überwachungen nach dem BÜPF nicht kostendeckend seien; ferner wurde geltend gemacht, dass die rechtliche Verpflichtung der Anbieterinnen, bestimmte, besonders auch neue Massnahme durchzuführen, nicht immer klar sei. Diese Themen sind indessen nicht im Rahmen des NDG zu behandeln, sondern in Rahmen der Totalrevision des BÜPF. Die gesetzlichen Auflagen an die Anbieterinnen, die Überwachungsfähigkeiten technisch zu gewährleisten sind eine Folge der staatlichen Erlaubnis, in einem wichtigen und lukrativen Geschäftsbereich des Service public tätig zu sein.

Die zusätzlich zu erwartenden Überwachungen des NDB verursachen beim Dienst ÜPF einen relativ geringen Mehraufwand im Vergleich zu den heute schon bestehenden Leistungen für die Strafverfolgungsbehörden (2011: 2699 Massnahmen zur Überwachung in Echtzeit, 5758 rückwirkende Überwachungsmassnahmen/Randdaten und 3918 technisch-administrative Auskünfte[25]).

Buchstabe b regelt den Einsatz von technischen Mitteln wie GPS-Geräten, mit denen der Standort einer Person, eines Fahrzeugs oder einer anderen beweglichen Sache

24 Vgl. BBl **2013** 2789

25 Die Statistik, des Dienstes ÜPF kann im Internet abgerufen werden unter: www.li.admin.ch > Themen > Statistik

festgestellt werden kann. Dabei erfolgt die Aufzeichnung eines Bewegungsmusters oder die Übertragung eines Signals, mit dem der Standort des Senders und damit der Person, des Fahrzeugs oder der beweglichen Sache festgestellt und gegebenenfalls aufgezeichnet werden kann. Diese technischen Mittel dienen unter anderem der Unterstützung von Observationsmassnahmen (analog den polizeilichen Einsätzen, bei denen die Verwendung seit Jahren gängige Praxis ist). Sie können diese Einsätze unterstützen (z.B. bei Verlust des Kontakts zum Zielobjekt), aber auch teilweise ersetzen (wenn keine direkte Beobachtung notwendig ist) oder vorbereiten (Kennenlernen der Gewohnheiten des Zielobjekts, womit gezieltere Einsätze der Observationsteams ermöglicht werden).

Um künftige technische Entwicklungen nicht auszuschliessen, ist die Definition der einzusetzenden Geräte dabei bewusst offen formuliert.

Wird die Ortung eines Mobiltelefons über Daten der Anbieterin vorgenommen, liegt eine Überwachung des Fernmeldeverkehrs nach dem BÜPF vor, die unter Buchstabe a fällt.

Buchstabe c ermöglicht insbesondere die Aufnahme von Gesprächen von überwachten Personen in Privaträumen und deren bildliche Überwachung (Videotechnik). Nach dem geltenden Recht ist eine solche Überwachung ausserhalb von Strafverfahren nicht zulässig. Wenn konkrete Anhaltspunkte für schwerwiegende sicherheitsbedrohende Handlungen von bestimmten Personen vorliegen, muss der NDB in der Lage sein, seine Abklärungen auch auf private Räume auszudehnen. Es gelten auch hier die Grundsätze nach Artikel 26.

Nachfolgend ein Beispiel für den möglichen Einsatz von technischen Überwachungsmassnahmen: Wo kleine terroristische Zellen bestehen (z.B. die Dreierzelle des nationalsozialistischen Untergrunds in Deutschland), finden Kontakte nur konspirativ im Untergrund statt. In der Öffentlichkeit äussern solche Personen ihre Absichten nicht. Sie haben somit keine Kontakte zu aussenstehenden Personen, denen sie ihre Absichten und Vorbereitungen kundgeben. In solchen Kreisen können folglich auch keine menschlichen Quellen eingesetzt werden, da diese Zellen keinen Zugang von aussen erlauben. Nur durch technische Überwachungsmittel können diejenigen Informationen beschafft werden, die benötigt werden, um Sicherheitsgefährdungen wie terroristische Anschläge zu verhindern. Wenn die Schwelle zum Verdacht auf strafbare Handlungen überschritten wird, schaltet der NDB die Strafverfolgungsbehörden ein (Art. 59).

Buchstabe d trägt der zunehmenden Verlagerung von sicherheitsbedrohenden Aktionen und Äusserungen ins Internet und dort in zugriffsgeschützte Bereiche Rechnung. Der NDB benötigt in Anbetracht der zunehmend aus dem Internet erwachsenden Bedrohungen für die Sicherheit der Schweiz neue, adäquate Mittel, um im Rahmen seiner präventiven Aufgabe die Netzwerke aufklären und die Bedrohung beurteilen zu können. Es geht dabei einerseits um das Beschaffen von Informationen (Ziff. 1) und andererseits um die Störung, Verhinderung oder Verlangsamung des Zugriffs auf Informationen (Ziff. 2), wenn es zu Angriffen auf kritische Infrastrukturen kommt.

Der NDB ist zur Aufdeckung und Beurteilung von wichtigen sicherheitsbedrohenden Entwicklungen darauf angewiesen, dass er gegebenenfalls auch in besonders gesicherte Netzwerke eindringen kann. Die daraus gewonnenen Informationen können beispielsweise dazu beitragen, geplante Aktivitäten terroristischer Art aufzudecken und zu verhindern.

Störungen von kritischen Infrastrukturen können die innere oder äussere Sicherheit der Schweiz auf gravierende Weise bedrohen und beinhalten ein riesiges Schadenspotenzial. Zu denken ist etwa an elektronische Angriffe auf die Energieversorgung (z.B. Atomkraftwerke), Transport und Verkehr (z.B. Luftfahrt, Schienen- und Strassenverkehr), die chemische Industrie (z.B. Sondermüll), die Telekommunikation (z.B. Radio und Fernsehen), das Gesundheitswesen (z.B. medizinische Versorgung) oder das Finanz- und Versicherungswesen (z.B. Börsen). Ziffer 2 soll somit die Abwehr von unmittelbar drohendem Schaden oder, während eines laufenden Angriffs, von bereits ganz oder teilweise eingetretenem Schaden ermöglichen. Vorbehalten bleibt das Subsidiaritätsprinzip, indem der NDB nur im Sinne einer «ultima ratio» aktiv wird, d.h. allfällige Strafverfahren gehen vor und der NDB könnte nur tätig werden, wenn die Voraussetzungen für ein Strafverfahren (noch) nicht gegeben oder ein solches für die Abwehr eines tatsächlichen Angriffs aussichtslos sind. Hier muss der präventive Schutz des Landes (z.B. vor atomarer Verseuchung) vorgehen. Zu betonen bleibt, dass Abwehrmassnahmen gegen Systeme im Inland nach Ziffer 2 immer genehmigungspflichtig sind, also sowohl gerichtlicher Genehmigung (Zustimmung des Bundesverwaltungsgerichts) als auch politischer Genehmigung (Freigabe durch die Chefin oder den Chef des VBS) bedürfen.

Im EJPD befasst sich die Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) mit dem strafrechtlichen Aspekt von Internet-Aktivitäten.

Mit *Buchstabe e* wird neu vorgeschlagen, dem NDB in wichtigen Fällen die richterlich und politisch kontrollierte Möglichkeit zu geben, Räumlichkeiten, Fahrzeuge und Behältnisse zu durchsuchen, um sicherheitsbedrohende Informationen oder Gegenstände (z.B. Dokumente) zu beschaffen. Dabei kann es sich um Taschen, Koffer, Container, Datenträger oder Aufzeichnungsgeräte wie Kameras und Diktaphone handeln. An Personen selbst darf der NDB weiterhin keine Untersuchungen durchführen. Dies soll den Polizeiorganen vorbehalten bleiben.

Siehe auch Erläuterungen zu Art. 25 Abs. 1 Bst. a und a^{bis} (NDG) unter «Koordination mit der Totalrevision des BÜPF» (Änderung anderer Erlasse)

Absatz 2 bestimmt, dass die vorstehenden Massnahmen verdeckt und ohne Kenntnis der betroffenen Personen durchgeführt werden. Dies ist notwendig, um den angestrebten Erfolg der Massnahmen nicht zu vereiteln. Im Gegenzug sichert ein doppeltes, richterliches und politisches Genehmigungsverfahren die rechtsstaatliche Überprüfung der Massnahmen. Ausserdem erfolgt eine nachträgliche Mitteilung (Art. 32) mit der Möglichkeit, gegen die Anordnung der Massnahmen Beschwerde zu führen (Art. 79).

Heute können sich Angehörige von fremden Nachrichtendiensten oder Terrornetzwerken in der Schweiz bei der Kommunikation sicher fühlen vor nachrichtendienstlicher Früherkennung, was auch entsprechend ausgenutzt wird. Künftig sollte schon die verbesserte Schweizer Aufklärungsfähigkeit hier mehr Zurückhaltung bewirken und auch fremde Dienste davon zurückhalten, auf eigene Faust tätig zu werden.

Art. 26 Grundsatz

Absatz 1 knüpft den Einsatz genehmigungspflichtiger Beschaffungsmassnahmen zunächst an die (alternativen) Voraussetzungen, dass eine konkrete Bedrohung der inneren oder äusseren Sicherheit vorliegt (mit Ausnahme des gewalttätigen Extremismus) oder dass aufgrund eines Bundesratsbeschlusses wesentliche Landes-

interessen nach Artikel 3 wahrgenommen werden. Der Bundesrat legt in seinem Beschluss auch fest, unter welchen Voraussetzungen genehmigungspflichtige Beschaffungsmassnahmen zum Einsatz kommen können. Das Genehmigungsverfahren richtet sich aber in jedem Fall nach den Artikeln 28 ff., das heisst der Beschluss des Bundesrates ersetzt dieses nicht, ist aber eine formelle Voraussetzung für die Anordnung, wenn nicht eine konkrete Bedrohung im vom Gesetz einschränkend definierten Sinne vorliegt.

Sowohl beim Vorliegen wesentlicher Landesinteressen als auch bei einer konkreten Bedrohung der inneren oder äusseren Sicherheit nach Artikel 19 Absatz 2 Buchstaben a–d müssen (kumulativ) folgende zusätzlichen Voraussetzungen erfüllt sein, damit eine genehmigungspflichtige Beschaffungsmassnahme eingesetzt werden kann:

- Die Schwere der Bedrohung der Sicherheit der Schweiz muss die Massnahme rechtfertigen.
- Die bisherigen nachrichtendienstlichen Abklärungen waren entweder erfolglos oder die Abklärungen wären ohne die besondere Beschaffungsmassnahme aussichtslos oder würden unverhältnismässig erschwert.

Diese zusätzlichen, einschränkend umschriebenen Anforderungen des verfassungsmässigen Verhältnismässigkeitsprinzips sind denjenigen im Strafprozessrecht nachgebildet (vgl. Art. 269 Abs. 1 StPO). Nicht ausreichend ist also auch, wenn eine Organisation oder Gruppierung auf der Beobachtungsliste nach Artikel 71 aufgeführt ist. Dies kann ein Indiz für die Schwere der Bedrohung der inneren Sicherheit sein, jedoch muss die Schwere im konkreten Einzelfall für die Massnahme ebenso nachgewiesen werden wie die Notwendigkeit nach Buchstabe c.

Der gewalttätige Extremismus soll von diesen Beschaffungsmassnahmen ausgenommen sein. Der Bundesrat ist der Auffassung, dass dies gerechtfertigt ist, da gewalttätiger Extremismus näher an politisch-ideologischen Bewegungen angesiedelt ist, was besondere Zurückhaltung erfordert. Wenn sich hingegen gewalttätiger Extremismus zum Terrorismus hin entwickelt, wird eine Überwachung unter diesem Aspekt möglich. Die jährliche Bestimmung der gewalttätig-extremistischen Gruppierungen durch den Bundesrat gemäss Artikel 69 des Entwurfs stellt dabei die politische Steuerung sicher und verhindert, dass der NDB selbstständig gewalttätig-extremistische Gruppierungen dem terroristischen Lager zuweisen kann.

Beauftragte Drittstellen nach *Absatz 3* werden in der Praxis vor allem der Dienst ÜPF im EJPD für die mit Fernmeldeüberwachungen zusammenhängenden Massnahmen sein, aber auch die Sicherheitsorgane der Kantone für den Einsatz von technischen Überwachungsgeräten oder bei Durchsuchungen.

Art. 27 Anordnung von genehmigungspflichtigen Beschaffungsmassnahmen gegenüber Drittpersonen

Es kommt vor, dass eine Person, bei der die Voraussetzungen nach Artikel 26 Absatz 1 für die Anordnung einer genehmigungspflichtigen Massnahme gegeben sind, für die Übermittlung und den Empfang von Informationen das Telefon, die Postadresse, den Computer, das Fahrzeug oder eine andere Einrichtung einer Drittperson benützt. Dies kann mit oder ohne Kenntnis derselben geschehen. In diesen Fällen soll der NDB die Möglichkeit erhalten, den Post- und Telefonverkehr der Drittperson überwachen zu lassen, auf deren Computer Zugriff zu nehmen oder

deren Räumlichkeiten und Fahrzeuge zu durchsuchen, um die Informationen über die Person zu erhalten, die das eigentliche Ziel der Überwachung ist. Die Privatsphäre der Drittperson wird dabei bestmöglich geschützt, und die Drittperson wird nach Beendigung der Massnahme über dieselbe orientiert (Art. 32).

Nicht zulässig ist die Überwachung von Drittpersonen, die nach den Artikeln 171–173 StPO ein Zeugnisverweigerungsrecht besitzen, z.B. Geistliche, Rechtsanwälte, Medizinalpersonen und deren Hilfspersonen oder Medienschaffende. Hier folgt das NDG ebenfalls den Regelungen der StPO. Eine Ausdehnung auf weitere Berufsgruppen, wie vereinzelt in der Vernehmlassung vorgeschlagen (z.B. Finanzdienstleister), wäre eine rechtspolitisch weitreichende Neuerung, für die der Bundesrat derzeit keine Notwendigkeit erkennt. Diese mögliche Neuerung müsste umfassender diskutiert werden, als dies im Rahmen des NDG möglich ist.

Art. 28 Genehmigungsverfahren

Das hier vorgeschlagene Genehmigungsverfahren ist zweistufig: Der NDB muss in einem ersten Schritt die Genehmigung durch eine Gerichtsinstanz, namentlich das Bundesverwaltungsgericht, einholen. Nur wenn dieses die richterliche Genehmigung der Massnahme erteilt hat, erfolgt in einem zweiten Schritt die Beurteilung und Freigabe der Massnahme aus politischer Sicht durch die Chefin oder den Chef des VBS (Art. 29), die oder der vorgängig dazu den Sicherheitsausschuss des Bundesrates konsultiert.

Im Einzelnen gestaltet sich das Vorgehen wie folgt:

1. Der NDB stellt dem Bundesverwaltungsgericht einen Antrag auf Einsatz einer genehmigungspflichtigen Beschaffungsmassnahme.
2. Die Präsidentin oder der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts prüft den Antrag und entscheidet, ob die beantragte Massnahme genehmigt oder abgelehnt wird bzw. kann die Akten ergänzen lassen.
3. Bei Genehmigung der Massnahme entscheidet die Chefin oder der Chef des VBS anschliessend über die Freigabe zur Durchführung.
4. Danach kann der NDB die Massnahme vollziehen oder beauftragten Dritten (z.B. dem Dienst ÜPF) eine Anordnung zustellen.

Der Antrag enthält alle notwendigen Angaben zur Beurteilung, ob die Massnahme den gesetzlichen Anforderungen entspricht, also namentlich die Beschreibung der tatsächlichen Anhaltspunkte für die konkrete Bedrohung der inneren oder äusseren Sicherheit der Schweiz, die Darlegung der Verhältnismässigkeit der Massnahme, die Bezeichnung der zu überwachenden Zielperson, soweit diese bereits identifiziert ist, ferner die einzusetzenden Mittel und allfällige Schutzmassnahmen zur Wahrung der Persönlichkeitsrechte der überwachten Person oder von Dritten. Analog zur StPO hat die Präsidentin oder der Präsident der zuständigen Abteilung den Entscheid kurz zu begründen. Das Verwaltungsgerichtsgesetz sieht in Artikel 23 Entscheide durch Einzelrichter vor (vgl. auch Änderungen anderer Erlasse, Ziff. 5).

Das Bundesverwaltungsgericht ist deshalb die richtige Instanz, weil es schon heute mit der rechtlichen Überprüfung von Massnahmen mit sicherheitspolitischen Hintergründen beauftragt ist, zum Beispiel bei der Beurteilung von Beschwerden bezüglich Einreiseverbote gegen Ausländerinnen und Ausländer aus Gründen der inneren

oder äusseren Sicherheit. Das in der Vernehmlassung vereinzelt vorgeschlagene Bundesstrafgericht hat jedoch bei der Anwendung strafrechtlicher Kriterien bei entsprechenden Verdachtslagen einen ganz anderen Fokus als das Bundesverwaltungsgericht. Der Bundesrat will deshalb auch beim Genehmigungsverfahren die Trennung von Nachrichtendienst und Strafverfolgung einhalten.

Die Genehmigung wird analog zu Artikel 274 Absatz 5 StPO für höchstens drei Monate erteilt, wobei sie mehrmals um jeweils höchstens drei Monate verlängert werden kann. Erweist sich eine Verlängerung als notwendig, so stellt der NDB einen Verlängerungsantrag mit den gleichen Angaben, wie sie für die Genehmigung notwendig sind (Abs. 5). Bei der Prüfung der Genehmigung von Verlängerungen wird die Gesamtdauer der Massnahme im Rahmen der Verhältnismässigkeitsprüfung gegen andere Faktoren wie die Schwere und Konkretheit der Bedrohung abzuwägen sein.

Dieses Verfahren soll dem Umstand Rechnung tragen, dass durch den Einsatz von genehmigungspflichtigen Beschaffungsmassnahmen Eingriffe in Grundrechte stattfinden können, ohne dass die überwachte Person davon Kenntnis hat und ohne dass sie sich während der Dauer der Massnahme dagegen wehren kann.

Erkenntnisse aus genehmigungspflichtigen Beschaffungsmassnahmen unterliegen gegenüber den Strafverfolgungsbehörden besonderen Verwertungsregeln; damit wird verhindert, dass die Überwachungsmassnahmen für Straffälle verwendet werden, in denen keine vergleichbare strafprozessuale Ermittlungsmassnahme zulässig gewesen wäre (vgl. Art. 59 Abs. 3 und 4).

In der Vernehmlassung war vereinzelt vorgeschlagen worden, die richterliche Genehmigung erst nach der politischen einzuholen, damit der Richter sich nicht mit politisch aussichtslosen Anordnungen befassen muss und sich die politischen Entscheidträger nicht allein auf die rechtliche Beurteilung verlassen. Der Bundesrat ist indessen der Auffassung, dass der ursprüngliche Vorschlag weiterzuverfolgen ist. Beim umgekehrten Verfahren müssten sich drei Bundesräte vor einem Einzelrichter mit einem möglicherweise gesetzeswidrigen Antrag befassen. Zudem könnte argumentiert werden, dass ein Einzelrichter sich befangen fühlen könnte, gegen die Empfehlung des Sicherheitsausschusses und den Entscheid der Chefin oder des Chefs des VBS einen ablehnenden Entscheid zu fällen. Grossmehrheitlich wurde das in der Vernehmlassung vorgeschlagene Genehmigungsverfahren denn auch begrüsst.

Art. 29 Freigabe

Dieser Artikel regelt die bereits erwähnte Freigabe einer richterlich bewilligten genehmigungspflichtigen Beschaffungsmassnahme durch die Chefin oder den Chef des VBS, die oder der vorgängig den Sicherheitsausschuss des Bundesrates konsultiert. Dieses zweistufige Verfahren bewirkt, dass der Einsatz von solchen Massnahmen, die stark in die Grundrechte eingreifen, nicht nur nach rechtlichen, sondern auch nach politischen Gesichtspunkten beurteilt wird. Die sicherheitspolitische Führung hat hierbei ein weites politisches Ermessen, von einer Freigabe abzusehen.

Es ist jedoch zu betonen, dass die Chefin oder der Chef des VBS nur bereits richterlich genehmigte Massnahmen freigeben kann. Sie oder er kann keine Massnahme freigeben, deren Genehmigung nicht erteilt wurde.

Die Stellvertretung der Chefin oder des Chefs VBS erfolgt gemäss Artikel 22 des RVOG durch ein anderes Mitglied des Bundesrates. Eine Delegation innerhalb des Departements ist nicht möglich.

Art. 30 Verfahren bei Dringlichkeit

Im Gegensatz zu den Strafverfolgungsbehörden, die beispielsweise eine Post- und Telefonüberwachung sofort vollziehen und die Genehmigung nachträglich einholen (vgl. Art. 274 Abs. 1 StPO), muss der NDB bei Massnahmen nach den Artikeln 25 ff. grundsätzlich zuerst die Genehmigung durch das Bundesverwaltungsgericht und die Freigabe durch die Chefin oder den Chef des VBS, die oder der vorgängig den Sicherheitsausschuss konsultiert hat, einholen.

Artikel 30 sieht bei drohender Gefahr die Möglichkeit vor, dass der NDB umgehend Massnahmen nach den Artikeln 25 ff. ergreifen kann. Ein solcher Fall besteht immer dann, wenn nur ein sofortiges Handeln die rechtzeitige Feststellung der Tatsachen oder die Beobachtung von Aktivitäten erlaubt.

Wird beispielsweise dem NDB gemeldet, dass sich eine wichtige terroristische oder nachrichtendienstliche Zielperson auf einem Flug nach Zürich befindet und in drei Stunden dort landet, können unter Umständen nur sofort vollzogene genehmigungspflichtige Beschaffungsmassnahmen (z.B. Überwachung des Mobiltelefons, verdeckte Durchsuchung des Gepäcks, Bestückung mit einem Ortungsgerät) die Beschaffung der notwendigen Informationen für die Beurteilung der aktuellen Bedrohung ermöglichen. Hinterher besteht kaum mehr die Möglichkeit, versäumte Beschaffungen nachzuholen.

Die Chefin oder der Chef des VBS hat folgende Möglichkeiten, den Einsatz einer dringlich angeordneten Massnahme zu stoppen:

- Sie oder er kann den Einsatz der Massnahme schon nach der Orientierung durch den NDB abbrechen lassen.
- Sie oder er kann nach dem Erteilen der Genehmigung durch das Bundesverwaltungsgericht die Freigabe ablehnen (vgl. Art. 32). Dies ist dann denkbar, wenn sie oder er die Gesamtumstände des Einsatzes gemäss dem schriftlichen Antrag zur Kenntnis genommen hat, während die erste Information summarischer Natur ist.

Art. 31 Beendigung der genehmigungspflichtigen Beschaffungsmassnahme

Die Regelungen bei der Beendigung der genehmigungspflichtigen Beschaffungsmassnahmen entsprechen dem üblichen Standard (vgl. Art. 275 StPO). *Absatz 1 Buchstabe b* verhindert dabei im Sinne einer Verdeutlichung des Verhältnismässigkeitsprinzips, dass eine Massnahme länger angewendet wird als tatsächlich notwendig.

Durch die Mitteilung an die Genehmigungsinstanzen nach *Absatz 4* wird sichergestellt, dass auch diese immer auf dem Laufenden sind, welche Massnahmen aktuell noch in Vollzug stehen.

Art. 32 Mitteilungspflicht

Die Pflicht, Betroffene nachträglich über nachrichtendienstliche Massnahmen zu informieren, ergibt sich aus dem Schutz des Privatlebens einer Person und der Achtung der Privatsphäre. Diese Garantie gründet in Artikel 8 der Konvention vom 4. November 1950[26] zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) und Artikel 13 Bundesverfassung (BV).

Ist eine Operation bzw. ein zusammenhängender Vorgang aus möglicherweise mehreren Beschaffungsmassnahmen bezüglich eines bestimmten Sachverhalts beendet, muss der NDB die Personen, die Ziel der Massnahme waren, und Drittpersonen, deren Anschlüsse allenfalls überwacht wurden, grundsätzlich innerhalb eines Monats über die Informationsbeschaffung unterrichten *(Absatz 1)*. Das Gesetz knüpft hier nicht an die einzelne Massnahme an, weil beispielsweise gleichzeitig noch andere genehmigte Beschaffungsmassnahmen hängig sind und diese durch die Mitteilung einer bereits abgeschlossenen Massnahme gefährdet werden könnten (typisches Beispiel: Die Beschaffung der Randdaten zurückliegender Fernmeldeverbindungen nach Art. 25 Abs. 1 Bst. c ist mit der Weitergabe der Daten abgeschlossen, während gleichzeitig noch eine Überwachung des laufenden Fernmeldeverkehrs stattfindet). Es kann oft auch erst nach Abschluss aller Massnahmen beurteilt werden, ob eine Mitteilung möglich ist oder ob eine Ausnahme nach Absatz 2 notwendig ist (z.B. weil der Fall an die Strafverfolgungsbehörden überwiesen und damit ein rechtliches Verfahren ausgelöst wird). Mit der Mitteilung erfolgt eine Erläuterung der Beschwerdemöglichkeit nach Artikel 79.

Die Mitteilungspflicht gilt nicht für die Funk- und die Kabelaufklärung (Art. 36 – 42), da diese nicht auf die Fernmeldeanschlüsse von Personen ausgerichtet sind, sondern auf die Aufklärung von sicherheitspolitisch bedeutsamer Informationen in Funkausstrahlungen oder Kabelübermittlungen aus dem Ausland. Dort sind mithin nicht Personen oder deren umfassender Fernmeldeverkehr das Ziel der Beschaffungsmassnahmen.

Absatz 2 Buchstabe a nimmt Bezug auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, der im Urteil Klass gegen die Bundesrepublik Deutschland vom 6. September 1978 feststellte, dass eine nachträgliche Mitteilung den langfristigen Zweck einer Überwachung in Frage stellen würde und deshalb unter bestimmen Voraussetzungen unterlassen werden dürfe. Er hielt unter anderem Folgendes fest:

«… Eine nachträgliche Benachrichtigung jeder Person, die einmal von einer inzwischen aufgehobenen Maßnahme betroffen worden ist, könnte sehr wohl den langfristigen Zweck gefährden, der seinerzeit die Anordnung ausgelöst hat. Wie das BVerfG richtig festgestellt hat, könnte eine solche Bekanntgabe außerdem zur Aufdeckung von Arbeitsweise und Beobachtungsfeldern der Geheimdienste führen und möglicherweise sogar zur Identifizierung ihrer Agenten beitragen. Insoweit der sich aus den angefochtenen Vorschriften ergebende ‹Eingriff› nach Artikel 8 Absatz 2 [EMRK] gerechtfertigt ist […], kann es nach Ansicht des Gerichtshofes mit dieser Bestimmung nicht unvereinbar sein, dass der Betroffene nach Beendigung der Überwachungsmaßnahme nicht unterrichtet wird, da es gerade dieser Umstand ist, welcher die Wirksamkeit des ‹Eingriffs› sicherstellt.»

26 SR **0.101**

Buchstabe b stellt auf die auch von der EMRK respektierten überwiegenden öffentlichen Interessen an der Wahrung der inneren oder äusseren Sicherheit ab. Hier geht es auch darum, sicherheitsbedrohenden Kreisen keinen Aufschluss über die Abwehrtätigkeiten der Schweiz zu geben. So wird ein von der Schweiz aus operierender Somalier, welcher Freiwillige in der Schweiz für Dschihad-Reisen rekrutiert, aus naheliegenden Gründen nicht nachträglich über die Abhöraktion informiert.

Buchstabe c nimmt den Grundsatz des Schutzes berechtigter Interessen Dritter auf. So kann beispielsweise von der Mitteilung einer Überwachung an eine Drittperson abgesehen werden, wenn dadurch die eigentliche Zielperson der Überwachung kompromittiert würde.

Buchstabe d nimmt Bezug auf die Situation, dass der Aufenthaltsort der betroffenen Person oder der Drittperson nur mit unverhältnismässigem Aufwand in Erfahrung gebracht werden könnte oder dass der Aufenthaltsort zwar bekannt ist, die betroffene Person dort aber nur mit unverhältnismässigem Aufwand erreicht (namentlich im Ausland) oder durch eine formelle Mitteilung von Schweizer Behörden sogar gefährdet werden könnte.

Gemäss *Absatz 3* gilt für den Aufschub und den Verzicht auf die nachträgliche Mitteilung das gleiche Verfahren wie für die Anordnung der genehmigungspflichtigen Beschaffungsmassnahme selbst: Genehmigung durch das Bundesverwaltungsgericht und anschliessend Freigabe durch die Chefin oder den Chef des VBS (Art. 29).

Art. 33 Zusammenarbeit und Beauftragung in der Beschaffung

Heute sind staatliche und nichtstaatliche Akteurinnen und Akteure in den Bereichen Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus, verbotener Handel mit Waffen, chemischen, biologischen und nuklearen Massenvernichtungswaffen sowie Akteurinnen und Akteure im Bereich verbotener Technologietransfer global aktiv, sie halten sich nicht an zwischenstaatliche Grenzen oder Konventionen. Diese Akteurinnen und Akteure nutzen z.B. die visabefreite Schengenzone, um sich konspirativ in anderen Ländern zu treffen und somit den Überwachungsmassnahmen in den eigenen Ländern zu entgehen. Die Nachrichtendienste vieler Länder sind mit denselben grenzüberschreitenden Problemen konfrontiert und können die notwendigen Informationen oftmals nicht mehr alleine beschaffen.

Deshalb wird die Zusammenarbeit nach *Absatz 1* mit in- und ausländischen Behörden immer wichtiger, vor allem in den Bereichen der Informationsweitergabe, von grenzüberschreitenden Observationen, gemeinsamen Beschaffungsoperationen und technischen Überwachungsmassnahmen. Letztere werden nach geltendem schweizerischem Recht durchgeführt. Der NDB darf namentlich nicht auf dem Weg der Zusammenarbeit mit ausländischen Amtsstellen die Bestimmungen für genehmigungspflichtige Beschaffungsmassnahmen umgehen.

Unter *Absatz 2* fällt die ausnahmsweise Beauftragung von Privaten, die die Möglichkeit haben, auch mittels Bild- und Tonaufnahmen Informationen zu beschaffen. Voraussetzung für die Beauftragung ist, dass ohne den Einsatz dieser Privatpersonen eine Beschaffung der Information durch den NDB wesentlich erschwert oder gar unmöglich wäre. Beim Zugang zu einer bestimmten Personengruppe zur Nachrichtenbeschaffung kann beispielsweise der Einsatz einer Quelle (an Stelle einer Mitarbeiterin oder eines Mitarbeiters des NDB) zur Platzierung eines technischen Gerätes

einzig erfolgversprechend sein. Je unauffälliger eine Person sich in eine Umgebung einfügt, desto wahrscheinlicher wird der Beschaffungserfolg.

Unter die Beschaffungsmassnahmen im Sinne von *Absatz 2* können z.B. komplexe technische Überwachungsgeräte fallen, die nur von spezialisierten Privatfirmen betrieben werden. Denkbar ist auch der Einsatz von privaten Informatikspezialistinnen und Informatikspezialisten bei besonders geschützten Datennetzwerken.

Der NDB hat sich bei allen Beauftragten nach den Absätzen 1 und 2 zu vergewissern, dass diese den Auftrag gesetzeskonform erfüllen, und er hat diese bei der Auftragserfüllung ebenso eng zu beaufsichtigen, wie seine eigenen Mitarbeiterinnen und Mitarbeiter. Bei der Beauftragung wird er deshalb Punkte wie Geheimhaltung, Kontrollrechte des NDB und des EDÖB über die Verwendung der Daten, Verbot der Nutzung der Daten zu anderen Zwecken oder Massnahmen zur Informationssicherheit schriftlich regeln. Welche Regelungspunkte jeweils notwendig sind, richtet sich nach der Art des Auftrags.

Ausländische Amtsstellen werden vom NDB nicht formell beauftragt, sondern im Rahmen der Zusammenarbeit mit Ersuchen kontaktiert. Der Bundesrat legt dabei nach Artikel 69 Absatz 1 Buchstabe f jährlich die Zusammenarbeit mit ausländischen Behörden fest.

Für allfällige Ansprüche gilt das allgemeine Haftungsrecht des Bundes nach dem Verantwortlichkeitsgesetz vom 14. März 1958[27].

Art. 34 Quellenschutz

Die Wahrung des Quellenschutzes ist für einen Nachrichtendienst von grösster Bedeutung. Quellen sollen nur in Ausnahmefällen preisgegeben werden müssen, wenn das öffentliche Interesse an der Preisgabe weit überwiegt. Gewisse Quellen sind sogar rigoros zu schützen. Andernfalls würde das Vertrauen in die Diskretion des NDB beeinträchtigt und die Beschaffung von Informationen stark erschwert.

Das heutige Recht enthält in Artikel 7 ZNDG eine nur sehr rudimentäre Regelung zum Quellenschutz und delegiert den Schutz im Übrigen an den Bundesrat. Der Bundesrat ist der Auffassung, dass die umfassende Kodifizierung des Nachrichtendienstes auch eine ausführlichere Regelung des Quellenschutzes enthalten muss. Damit sollen allfällige Widersprüche zwischen speziellem Verordnungsrecht und gesetzlichen Bestimmungen anderer Erlasse vermieden werden.

Absatz 1 definiert den Grundsatz des Quellenschutzes und der schon bisher in Artikel 7 ZNDG aufgeführten besonderen Schutzwürdigkeit der Personen, welche Informationen über das Ausland beschaffen. Darunter fallen aber auch die Beziehungen zu ausländischen Nachrichtendiensten und Sicherheitsbehörden, ohne deren umfassenden Schutz die Schweiz als unsichere Partnerin betrachtet würde. Dies könnte schwere Folgen für die Vertrauenswürdigkeit des NDB als Kooperationspartner haben. Keinen Schutz hätten allerdings Personen verdient, die wegen Verbrechen gegen die Menschlichkeit (Art. 264 und 264*a* StGB) oder Kriegsverbrechen (Art. 264*b*–264*j*) beschuldigt sind. Hier gilt der Quellenschutz nicht, wenn gegen die Person ein Verfahren eines Schweizer Gerichts oder eines von der Schweiz anerkannten internationalen Gerichts eröffnet wurde. Der Quellenschutz gilt auch nicht, wenn die Schweiz zur internationalen Rechtshilfe verpflichtet ist.

27 SR **170.32**

Absatz 2 beschränkt den Schutz menschlicher Quellen (Art. 15) im Inland gegenüber Strafverfolgungsbehörden. Diese Personen erhalten keinen Quellenschutz, wenn sie selbst eines Offizialdelikts beschuldigt werden oder wenn die Bekanntgabe ihrer Identität unerlässlich ist, um eine schwere Straftat aufzuklären. Zum Begriff der schweren Straftat gibt es im Straf- und Strafprozessrecht keine allgemeingültige formellgesetzliche Definition. Es gibt auch keine generell gültigen Kriterien für schwere Straftaten. Vielmehr spielt der Kontext für die Qualifikation einer Straftat eine Rolle. Als Anhaltspunkt dafür, was als schwere Straftat gilt, kann immerhin die Definition in Artikel 11 Absatz 3 der Zwangsanwendungsverordnung vom 12. November 2008[28] herangezogen werden:

[3] Als schwere Straftat gilt eine ernsthafte Beeinträchtigung gegen Leib und Leben, der Freiheit, der sexuellen Integrität oder der öffentlichen Sicherheit.

Absatz 3 führt daneben aus, welche Kriterien weiterhin für den Quellenschutz anzuwenden sind. Dabei steht jeweils der Fortbestand der Quelle zur Informationsgewinnung im Vordergrund. Gemäss der allgemeinen Regelung über den Erlass des Vollzugsrechts regelt der Bundesrat die Einzelheiten in einer Verordnung.

Der Bundesrat hält es für angebracht, dass das Gesetz für die Beurteilung von Streitigkeiten im Bereich des NDB eine einzige Instanz vorsieht, die das entsprechende Fachwissen für nachrichtendienstliche Belange entwickeln kann. Er schlägt deshalb in *Absatz 4* für den Quellenschutz das Bundesverwaltungsgericht als Entscheidinstanz vor. Der Verweis auf die Rechtshilfe beschlägt nur das innerstaatliche Verhältnis. Die internationale Rechtshilfe erfolgt über die zuständigen Justizbehörden und nicht durch den Nachrichtendienst.

Art. 35 Allgemeine Bestimmungen

Einleitende Bemerkungen

Die Beschaffung von Informationen über Vorgänge im Ausland basiert heute auf der allgemein gehaltenen Regelung nach Artikel 1 Buchstabe a ZNDG:

«Der Bundesrat bezeichnet die Dienststellen des Bundes, welche die Aufgaben des zivilen Nachrichtendienstes des Bundes erfüllen. Diese Dienststellen:

a. beschaffen sicherheitspolitisch bedeutsame Informationen über das Ausland und werten sie zuhanden der Departemente und des Bundesrates aus;»

Diese Regelung geht auf den früheren Artikel 99 Absatz 1 MG zurück. Sie wurde im ZNDG sehr allgemein gehalten, da dieses lediglich die bestehenden Rechtsgrundlagen zum zivilen Nachrichtendienst zusammenfassen wollte, ohne neue inhaltliche Schranken aufzustellen. Das ZNDG übernahm deshalb die Regelung des MG, das dem Nachrichtendienst betreffend die Informationsbeschaffung im Ausland einen grossen Spielraum gewähren und auch gegenüber dem Ausland die Methoden und Möglichkeiten der Informationsbeschaffung des Auslandnachrichtendienstes (damaliger SND) nicht offenlegen wollte.

Artikel 16 V-NDB umschreibt heute die im Ausland zulässigen Methoden der nachrichtendienstlichen Informationsbeschaffung genauer.

Wenn die Beschaffung von Auslandnachrichten im Inland erfolgt, gelten grundsätzlich dieselben Regeln wie für die Beschaffung über Vorgänge im Inland (Abs. 2).

[28] SR **364.3**

Die Nachrichtenbeschaffung im Ausland funktioniert hingegen nach anderen Regeln als diejenige im Inland. Der NDB setzt die Beschaffungsmassnahmen im Ausland in eigener Verantwortung ein, auch diejenigen, die im Inland genehmigungspflichtig sind (Art. 25 ff.).

Die unterschiedliche Regelung der Inland- und Auslandbeschaffung entspricht einer Praxis, die für die meisten Nachrichtendienste der Welt Gültigkeit hat und sich im Grunde aus der Tatsache ergibt, dass staatliche nachrichtendienstliche Informationsbeschaffungstätigkeiten in anderen Ländern von diesen Ländern in der Regel als Spionage beurteilt und strafrechtlich verfolgt werden. Spionagedelikte sind hingegen international nicht rechtshilfefähig. Der Bundesrat hält es deshalb für nicht sinnvoll, die Beschaffung im Ausland einem richterlichen oder politischen Genehmigungsverfahren zu unterstellen. Die Genehmigung könnte im Ausland ohnehin keine rechtliche oder politische Wirkung entfalten, sondern könnte aus der Sicht des Zielstaates als rechtswidriger Eingriff von schweizerischen richterlichen und politischen Behörden in die Souveränität des betreffenden Staates betrachtet werden. Im Weiteren ist Folgendes zu berücksichtigen:

- Bei der Informationsbeschaffung im Ausland wird der Kerngehalt der Grundrechte respektiert und der Eingriff in die Grundrechte von Personen auf das Notwendige beschränkt wird (Abs. 3).
- Die Beschaffungsaktivitäten betreffend Vorgänge im Ausland werden zuhanden der Aufsichts- und Kontrollorgane eng dokumentiert (Abs. 4).
- Die Informationsbeschaffung im Ausland unterliegt der Kontrolle durch das VBS, durch den Bundesrat und schliesslich durch die Geschäftsprüfungsdelegation (vgl. Art. 74 ff.).

Die im Gesetzesentwurf vorgesehenen Tätigkeiten des NDB erfolgen unter diesen Voraussetzungen konform mit den völkerrechtlichen Verpflichtungen der Schweiz.

Absatz 1 statuiert den Grundsatz, dass Beschaffungsaktivitäten im Ausland verdeckt durchgeführt werden. Dies ist notwendig, da sie ansonsten durch betroffene Staaten oder Akteure verhindert werden und sowohl Mitarbeiterinnen und Mitarbeiter als auch Quellen des NDB gefährdet werden könnten.

Absatz 2 erlaubt der Auslandsbeschaffung auch die Tätigkeit im Inland (z.B. die Durchführung von Treffen mit menschlichen Quellen), stellt aber sicher, dass der NDB dieselben Regeln einhält wie für die Beschaffung im Inland. Dies gilt insbesondere für die allfällige Anwendung genehmigungspflichtiger Beschaffungsmassnahmen (4. Abschnitt). Davon ausgenommen sind besondere Tätigkeiten nach Artikel 36 (Eindringen in fremde Computersysteme und -netzwerke im Ausland).

Der NDB setzt somit verdeckte Beschaffungsmassnahmen im Ausland in eigener Verantwortung ein, auch solche, die nach den Artikeln 25 ff. im Inland genehmigungspflichtig wären. Der Grund für die gegenüber der Inlandbeschaffung abweichende Regelung liegt neben den oben erwähnten Gründen auch darin, dass die mit der Beschaffung von Auslandnachrichten befassten Mitarbeiterinnen und Mitarbeiter des NDB eine grössere situative Handlungs- und Ermessensfreiheit in der Wahl der Mittel benötigen, um ihre Aufträge erfüllen zu können.

Der Bundesrat schlägt deshalb vor, die verdeckten Beschaffungsmassnahmen, die im Ausland zulässig sind, ohne besondere Genehmigung zu regeln. Dies weil Schweizer Gerichte im Regelfall weder die jeweiligen Verhältnisse vor Ort kennen, noch sich innert nützlicher Frist die für eine verantwortungsvolle Entscheidfindung not-

wendigen Informationen beschaffen können. Somit ist bei gegebener Sachlage kein ordentliches Genehmigungsverfahren (welches auf internationalem Parkett ohnehin ein Unikum wäre) möglich. Hinzu käme die Problematik, dass eines der höchsten Schweizer Gerichte im Voraus Handlungen für rechtmässig erklären würde, die in den Ländern, in welchen sie ausgeführt werden, meist als strafbar betrachtet werden. Aber auch in der Auslandsbeschaffung ist der Grundsatz der Verhältnismässigkeit zu beachten, wie *Absatz 3* ausdrücklich festhält. Die Grundrechtseingriffe dürfen auch im Ausland nicht in einem Missverhältnis zum erwarteten Informationsgewinn stehen. Der Kerngehalt der Grundrechte ist gemäss Bundesverfassung ohnehin durch alle Behörden zu wahren, was auch für den Nachrichtendienst in der Auslandsbeschaffung gilt.

Die vorwiegende Eigenverantwortung des NDB für die Beschaffungstätigkeiten im Ausland bedeutet indessen nicht den Wegfall einer wirksamen Kontrolle. Im Gegenteil: *Absatz 4* verpflichtet den NDB, die gesamte Beschaffung aller Informationen über Vorgänge im Ausland zuhanden der politischen Aufsicht des NDB durch den Bundesrat, das Parlament (Geschäftsprüfungskommission bzw. Geschäftsprüfungsdelegation) und das VBS (Nachrichtendienstliche Aufsicht) zu dokumentieren.

Im Ausland beschaffte Daten, die mit Hilfe von genehmigungspflichtigen Beschaffungsmassnahmen vergleichbaren Methoden beschafft wurden (z.B. durch den Einsatz von GPS-Ortungsgeräten), sind mit den Daten aus genehmigungspflichtigen Beschaffungsmassnahmen im Inland in Bezug auf Umfang, Geheimhaltungsbedürfnis und Sicherheitsrisiken (z.B. bezüglich Schadsoftware in Computerdaten) vergleichbar. Sie sollen deshalb gemäss *Absatz 5* gleich wie vergleichbare Daten aus der Inlandbeschaffung in gesonderten Informationssystemen abgespeichert werden können (vgl. Art. 57). Von dort können sie in verarbeiteter Form in andere Systeme überführt werden, wenn die Voraussetzungen für ihre Aufnahme gegeben sind. Dies wird vor allem das integrale Analysesystem IASA NDB betreffen (Art. 48).

Die im Ausland eingesetzten Mitarbeiterinnen und Mitarbeiter des NDB sind einem erhöhten Risiko ausgesetzt und bewegen sich auch in Kriegs- und in Krisengebieten, zum Teil unter Verwendung einer Legendierung und/oder einer Tarnidentität. Der Bundesrat schlägt in *Absatz 6* deshalb ihre Unterstellung unter die Militärversicherung vor.

Die in *Absatz 7* vorgesehenen Schutzmassnahmen können in Form von technischen Ausrüstungen, aber auch von Legendierungen und Tarnidentitäten oder operationeller Unterstützung bestehen, z.B. dem Einsatz von Gegenobservationen zur frühzeitigen Erkennung von Gefährdungen im Umfeld eines Einsatzes.

Art. 36 Eindringen in Computersysteme und -netzwerke

Artikel 36 regelt einige Sonderfälle der Beschaffung von sicherheitspolitisch relevanten Informationen über das Ausland. *Absatz 1* regelt das Eindringen von der Schweiz aus in Computersysteme und -netzwerke im Ausland zum Zweck des Störens, Verhinderns oder Verzögerns des Zugriffs auf Informationen (vgl. Art. 25 Abs. 1 Bst. d Ziff. 2). Erkenntnisse aus der strategischen Führungsübung 2013 haben gezeigt, dass solche Aktionen aussenpolitisch sensibel sein können und deshalb nicht in der alleinigen Zuständigkeit des NDB liegen können. Sie sollen deshalb nur auf Entscheid des Bundesrates durchgeführt werden und auch nur, wenn die entsprechenden ausländischen Systeme für Angriffe auf kritische Infrastrukturen verwendet

werden. Eine richterliche Genehmigung scheidet nach Auffassung des Bundesrates aus den bereits zu Artikel 35 ausgeführten Gründen aus.

Absatz 2 regelt hingegen das Eindringen von der Schweiz aus in Computersysteme und -netzwerke zur reinen Informationsbeschaffung (vgl. Art. 25 Abs. 1 Bst. d Ziff. 1), sofern sich diese Systeme und Netzwerke im Ausland befinden. Dabei muss der Gegenstand des Interesses der Aufklärung im Ausland situiert sein (beispielsweise Proliferationsprogramm eines ausländischen Staats). Da hier keine Systeme gestört oder in der Funktionsfähigkeit eingeschränkt werden, ist das Risiko aussenpolitischer Implikationen weit geringer als im Fall von Massnahmen nach Absatz 1. Der NDB soll deshalb diese auch von ausländischen Nachrichtendiensten intensiv praktizierte Beschaffung auch von der Schweiz aus in eigener Verantwortung durchführen. Sind allerdings besondere politische Risiken zu befürchten, muss die Direktorin oder der Direktor des NDB vorgängig die Zustimmung der Chefin oder des Chefs des VBS einholen.

Art. 37 Funkaufklärung

Die eidgenössischen Räte haben im Rahmen der Revision BWIS II im ZNDG mit Artikel 4*a* eine neue gesetzliche Bestimmung geschaffen, welche die nachrichtendienstliche Funkaufklärung erstmals auf dieser Stufe regelt. Diese Bestimmung trat nach der Anpassung der Verordnung vom 17. Oktober 2012[29] über die elektronische Kriegführung und die Funkaufklärung erst am 1. November 2012 in Kraft. Der Bundesrat hat sie deshalb weitestgehend unverändert in das Nachrichtendienstgesetz übernommen, mit kleinen Anpassungen an den Sprachgebrauch und den Geltungsbereich des NDG. So wurde neu in Absatz 2 die Wahrung wesentlicher Landesinteressen im direkten Auftrag des Bundesrates (vgl. Art. 3 und 70) in die möglichen Voraussetzungen für den Einsatz der Funkaufklärung aufgenommen.

Die Funkaufklärung ist auf das Ausland ausgerichtet, was bedeutet, dass sie nur Funksysteme, die sich im Ausland befinden, erfassen darf. In der Praxis betrifft dies vor allem Telekommunikationssatelliten und Kurzwellensender. Beim durchführenden Dienst handelt es sich um das Zentrum für elektronische Operationen der Schweizer Armee (ZEO). Nur dieses verfügt über die notwendigen technischen Anlagen. Absatz 4 stellt sicher, dass die Funksendungen nur nach Inhalten mit Auslandsbezug ausgewertet werden dürfen. Dabei können jedoch auch Informationen über Personen im Inland anfallen, namentlich wenn der Kommunikationspartner einer aufgeklärten ausländischen Person oder Einrichtung einen Schweizer Fernmeldeanschluss benützt. Solche Informationen darf das ZEO, sofern sie nicht auf eine konkrete Gefährdung der inneren Sicherheit hinweisen, nur anonymisiert an den NDB weiterleiten (Abs. 5). Das ZNDG verweist hier auf die weitere Bearbeitung nach den Regelungen des BWIS. Unter dem NDG sind darunter Bedrohungen nach Artikel 6 Absatz 1 Buchstabe a zu verstehen.

Die Funkaufklärung wird heute schon von der unabhängigen Kontrollinstanz (UKI) kontrolliert. Auch hier übernimmt der Bundesrat die entsprechende Regelung aus dem ZNDG (Art. 4*b*) weitgehend unverändert in Artikel 75 NDG. Gemäss Absatz 3 regelt der Bundesrat die weiteren Einzelheiten der Funkaufklärung. Dabei legt Absatz 3 nur den Mindestgehalt der Verordnungsregelungen fest. Wie bisher wird der Bundesrat auch weitere Bestimmungen in die Verordnung aufnehmen, wie

29 SR **510.292**

Regelungen über die Datenbearbeitung im durchführenden Dienst oder die Datensicherheit.

Damit übernimmt das NDG die neuen rechtlichen Regelungen und die Praxis des ZNDG und des BWIS. An deren Schaffung war im Rahmen der damaligen gesetzgeberischen Arbeiten Prof. Dr. iur. Giovanni Biaggini, Ordinarius für Staats-, Verwaltungs- und Europarecht an der Universität Zürich, im Auftrag der eidgenössischen Räte massgeblich beteiligt. Die vorliegende Bestimmung des NDG wie auch der folgende Abschnitt zur Kabelaufklärung wurden deshalb wiederum unter Beteiligung von Prof. Biaggini erarbeitet.

Art. 38 Allgemeine Bestimmungen

Neben der auch in der Schweiz schon heute praktizierten Funkaufklärung gewinnt international die Kabelaufklärung an Bedeutung. Diese ist wegen des höheren Regelungsbedarf in einem eigenen Abschnitt geregelt, gehört aber auch zur Beschaffung von Informationen über Vorgänge im Ausland. Eine Kabelaufklärung mit Fokus auf das Inland soll auch in Zukunft nicht zulässig sein.

Die Verlagerung der Fernmeldekommunikation von drahtlosen Mitteln (Funk) auf leitungsgebundene Netze (der Verständlichkeit halber hier als «Kabel» bezeichnet) hat sich in den letzten Jahren mit dem Ausbau der sehr leistungsfähigen Glasfasernetze intensiviert. Gleichzeitig nehmen die Möglichkeiten, Erkenntnisse aus der Funkaufklärung zu gewinnen, etwas ab. Der Vorentwurf orientierte sich deshalb teilweise an einer entsprechenden Gesetzgebung, die Schweden 2008 erlassen hatte (Gesetz 2008:717 über die Signalaufklärung im militärischen Nachrichtendienst; dieser hat in Schweden die Funktion des Auslandsnachrichtendienstes) und die auch die Kabelaufklärung regelt. Erst mit den notwendigen gesetzlichen Grundlagen ist es in der Schweiz möglich, nähere technische Abklärungen und Versuche mit der Kabelaufklärung durchzuführen. Aus dem Ausland ist bekannt, dass die Kabelaufklärung rein technisch machbar ist. Erst mit der Analyse der Datenströme durch die Schweiz lässt sich aber feststellen, ob mit der Kabelaufklärung auch in der Schweiz hinreichend nützliche Informationen gewonnen werden können. Schon für einen solchen Betrieb ist indessen eine formellgesetzliche Grundlage zwingend erforderlich.

Die Kabelaufklärung dient wie die Funkaufklärung der Informationsbeschaffung über das Ausland und ist deshalb nicht als genehmigungspflichtige Beschaffungsmassnahme im Inland konzipiert. Sollen ähnliche Aufklärungszwecke mit Bezug auf das Inland erreicht werden, wäre eine genehmigungspflichtige Beschaffungsmassnahme zu beantragen. Die Kabelaufklärung kann aber nur mit der Beteiligung schweizerischer Anbieterinnen von Fernmeldediensten durchgeführt werden, denen eine rechtsgültige Anordnung für das Weiterleiten der entsprechenden Datenströme an die ZEO übergeben werden muss. Da hier ein Beschwerdeverfahren durch die von der Aufklärungsmassnahme betroffenen Personen nicht möglich ist, sieht das Gesetz ein analoges Genehmigungsverfahren wie bei den genehmigungspflichtigen Beschaffungsmassnahmen im Inland vor (Art. 28). Die Bearbeitung der Daten erfolgt aber, anders als bei den genehmigungspflichtigen Beschaffungsmassnahmen, nicht in separaten Systemen, sondern – wie auch die Erkenntnisse aus der Funkaufklärung – im Restdatenspeicher und in IASA NDB (Art. 46 ff.).

Bei der Kabelaufklärung werden bestimmte Datenströme auf internationalen Fernmeldekabeln erfasst und ähnlich wie bei der Funkaufklärung nach Inhalten abge-

sucht, triagiert und der Auswertung zugeführt. Im Gegensatz zur Fernmeldeüberwachung im Inland als genehmigungspflichtige Beschaffungsmassnahme ist die Kabelaufklärung ein Mittel der Auslandsaufklärung. Diese ist nicht darauf ausgerichtet, den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zu erfassen; technisch ist dies auch nicht in der gleichen Art möglich wie bei der Fernmeldeüberwachung im Inland, da sich bei der Kabelaufklärung die Zielobjekte im Ausland befinden.

Für dieses Aufklärungsmittel bestehen in der Schweiz noch keine rechtlichen Grundlagen. Es handelt sich um eine für die Schweiz neue Form der auslandorientierten Aufklärung, die mit den Überwachungsformen im BÜPF nicht vergleichbar ist. Die Terminologien müssen und können deshalb nicht identisch sein und sie dürfen sich gerade nicht zu eng an bestehende technische Begriffe anlehnen, um weitere technische Entwicklungen nicht auszuschliessen.

Der durchführende Dienst nach *Absatz 1* ist wie bei der Funkaufklärung das ZEO. Dieses verfügt über die technische Kompetenz und die Einrichtungen zu deren Durchführung. Zum Schutz der Grundrechte der Personen, deren Kommunikationsdaten bei der Kabelaufklärung miterfasst werden, aber nicht den Suchkriterien des Auftrags des NDB entsprechen, ist es notwendig, dass nicht der NDB, sondern eine Drittstelle die Triage der Daten durchführt. Das ZEO leitet wie bei der Funkaufklärung nur an den NDB weiter, was einem Suchauftrag entspricht oder was direkte Hinweise auf eine Gefährdung der inneren oder äusseren Sicherheit enthält. Diese Kriterien und die Vorgehensweisen entsprechen weitgehend jenen bei der Funkaufklärung. Eine Beteiligung des Dienstes ÜPF im EJPD ist dabei weder notwendig noch sinnvoll, da es sich bei der Kabelaufklärung nicht um eine von diesem angebotene Überwachungsart nach dem BÜPF handelt. Das ZEO als durchführender Dienst tritt deshalb direkt mit den Betreiberinnen von leitungsgebundenen Netzen und den Anbieterinnen von Fernmeldediensten in Kontakt, um die Kabelaufklärung im konkreten Fall zu planen und zu vollziehen.

Absatz 2 stellt sicher, dass keine rein schweizerischen Kommunikationen erfasst werden. Wo dies technisch nicht möglich ist (z.B. kann der Leitweg von IP-Datenpaketen nicht vorausgesagt werden, auch wenn sich Absender/in und Empfänger/in in der Schweiz befinden), sind solche Daten unverzüglich zu vernichten, sobald ihre schweizerische Herkunft und Zieladresse erkannt werden. Diese Verpflichtung trifft sowohl das ZEO als auch den NDB.

Absatz 3 definiert Vorgaben an die Suchbegriffe, welcher der NDB für den Auftrag festlegt. Diese sollen möglichst präzis sein, damit möglichst wenige Daten erfasst und möglichst geringe Eingriffe in die Privatsphäre von Personen verursacht werden. Dies bedeutet, dass beispielsweise die Suche nach konkreten Personalien von ausländischen Terrorverdächtigen oder nach Fernmeldeanschlüssen, die diese verwenden, wirkungsvoller und schonender ist als die Verwendung eines trivialen Suchworts wie «Al-Qaïda» oder «Sprengstoffanschlag». Hierzu besteht bereits eine eingespielte, rechtlich korrekte und kontrollierte Praxis aus der Funkaufklärung.

Absatz 4 beauftragt den Bundesrat ähnlich wie Absatz 3 der Funkaufklärung mit dem Erlass des ausführenden Rechts in einer Verordnung.

Art. 39/40 Genehmigungspflicht / Genehmigungsverfahren

Diese Artikel regeln analog zu den genehmigungspflichtigen Beschaffungsmassnahmen die Genehmigung der Aufträge für die Kabelaufklärung. Weil hier Fernmeldeprovidern Anordnungen für die Weiterleitung bestimmter Datenströme zugestellt werden müssen und kein Widerspruchsverfahren durch die betroffenen Personen möglich ist, ist eine richterliche Überprüfung notwendig. Aus diesem Grund wird hier denn auch die UKI nicht tätig. Sonst würde eine Konkurrenz und Vermischung verschiedener Genehmigungs-, Kontroll- und Aufsichtsinstanzen entstehen.

Der Antrag nach Artikel 40 Absatz 1 umfasst auch die Kategorien von Suchbegriffen, nach welchen die Daten zuhanden des NDB auszuwählen sind. Die Erfahrung aus dem Betrieb der Funkaufklärung zeigt, dass diese Suchbegriffe dynamisch gehandhabt werden müssen und ständig verfeinert werden können. Deshalb ist auch bei der Kabelaufklärung vorgesehen, mit Kategorien von Suchbegriffen zu arbeiten, damit nicht bei jeder Verfeinerung eine neue Genehmigung eingeholt werden muss. Eine Kategorie von Suchbegriffen kann z.B. eine Gruppe von Angehörigen einer bestimmten Terrorgruppierung sein sowie die mit ihr in operativen Kontakten stehenden Personen. Diese Personen können namentlich erst im Verlauf der Aufklärung identifiziert werden. Präzise Suchbegriffe, die erst im Vollzug der Massnahme definiert werden, sind z.B. Angaben zu fernmeldetechnischen Adressierungselementen (z.B. Telefonnummern), Adressen oder Geschäfts- und Projektbezeichnungen.

Im Gegensatz zu den genehmigungspflichtigen Beschaffungsmassnahmen, welche jeweils nur für drei Monate genehmigt werden können, soll die Kabelaufklärung beim Erstauftrag nach *Absatz 3* für sechs Monate genehmigt werden können. Dies erscheint sinnvoll, da die Aufnahme der Erfassung und das Ausbilden und Einarbeiten der Mitarbeiterinnen und Mitarbeiter, die die Triage vornehmen, in einen Auftrag mehr Zeit erfordert als z.B. eine Fernmeldeüberwachung nach Artikel 25 Absatz 1 Buchstabe a (bei der dem NDB alle Kommunikationen zugeleitet werden). Für die Verlängerungen gilt dann wie bei den genehmigungspflichtigen Beschaffungsmassnahmen eine Frist von drei Monaten.

Art. 41 Durchführung

Die Durchführung gleicht dem Verfahren bei der Funkaufklärung, mit der Ausnahme, dass der durchführende Dienst bei der Kabelaufklärung die Signale der Fernmeldeeinrichtungen nicht selbst (mit Antennen) erfasst, sondern von den Fernmeldeprovidern zugeleitet erhält. Welche Provider betroffen sind, muss im Einzelfall anhand der Kenntnis der Durchleitungswege durch die Schweiz festgelegt werden.

Das weitere Verfahren und die Kriterien für die Auswahl der an den NDB weiterzuleitenden Daten orientieren sich sodann stark an den Regelungen für die Funkaufklärung (Abs. 2–5).

Zuständig für die nachrichtendienstliche Auswertung der Daten ist der NDB. Er entscheidet auch, welche Daten er gemäss den rechtlichen Grundlagen in seinen Informationssystemen ablegt und weiterbearbeitet (vgl. 4. Kapitel). Wie bisher kann das ZEO die weitergeleiteten Daten aber auch mit technischen oder inhaltlichen Erläuterungen, Zusammenfassungen oder Übersetzungen zuhanden des NDB versehen.

Art. 42 Pflichten der Betreiberinnen von leitungsgebundenen Netzen und der Anbieterinnen von Telekommunikationsdienstleistungen

Da wie bereits erläutert die Kabelaufklärung nur mit Beteiligung der Anbieterinnen von Fernmeldediensten und der Betreiberinnen von leitungsgebundenen Netzen betrieben werden kann, legt Artikel 42 deren Verpflichtungen fest. Verpflichtet sind dabei nur Betreiberinnen, die öffentliche Leistungen im Sinne des Fernmeldegesetzes vom 30. April 1997[30] (FMG) im grenzüberschreitenden Verkehr anbieten. Die technischen Auskünfte sind insbesondere auch notwendig, um die einzelnen Aufträge und die Anträge an die Genehmigungsinstanzen formulieren zu können. Ihre Erteilung ist deshalb nicht auf die konkrete Durchführung eines genehmigten und freigegebenen Auftrags beschränkt. In der Regel werden die technischen Fragen zwischen der durchführenden Stelle ZEO und den Providern zu klären sein. Der NDB braucht aber für die Begründung und Dokumentierung seiner Aufträge auch direkte Auskünfte von den Anbieterinnen von Fernmeldediensten und Betreiberinnen von leitungsgebundenen Netzen.

Eine Beteiligung des Dienstes ÜPF im EJPD ist dabei wie schon erwähnt nicht vorgesehen, da es sich bei der Kabelaufklärung nicht um eine von diesem angebotene Überwachungsart nach dem BÜPF handelt. Vielmehr müssen die technischen Modalitäten zwischen dem NDB, dem ZEO und den Betreiberinnen direkt und im Einzelfall geklärt werden.

Der Aufwand für die Realisierung der Kabelaufklärung lässt sich mangels Erfahrungen derzeit nicht abschätzen. So ist insbesondere nicht klar, welche nachrichtendienstlich relevanten Datenströme heute und in Zukunft überhaupt durch die Schweiz fliessen. Diese Informationen können – wie oben dargelegt – erst erhoben werden, wenn die entsprechenden gesetzlichen Grundlagen vorliegen.

Die Provider verlangten in der Vernehmlassung eine volle Entschädigung ihrer Kosten. Bei der aktuellen Revision des BÜPF wurde aber die aktuelle Regelung beibehalten (angemessene Entschädigung für die Nutzung der Überwachungsinfrastruktur der Provider im Anwendungsfall); dieser Grundsatz soll auch hier übernommen werden. Es besteht sonst namentlich kein Anreiz für die Provider, kostengünstige Lösungen zu suchen. Die konkrete Ausgestaltung der Entschädigungen auf Verordnungsebene wird mit den Providern diskutiert werden.

Der Bundesrat schätzt, dass die Aufnahme der konkreten Vorbereitungen für die Kabelaufklärung und erste Testbetriebe auf Seiten des NDB und des ZEO vorerst je zwei zusätzliche Stellen erfordern. Diese werden in den ordentlichen Personalplanungen beantragt werden.

4. Kapitel, 1. Abschnitt

Zur Aufgabenerfüllung nach diesem Gesetz, dem rechtzeitigen Erkennen und umfassenden Beurteilen von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz, ist der NDB wie jeder Nachrichtendienst auf eine breit angelegte Informationsbasis aus vielfältigen Quellen angewiesen.

Terroristische Anschläge, Spionageaktivitäten, gewalttätig-extremistische Aktionen usw. werden typischerweise verdeckt vorbereitet und so lange wie möglich geheim gehalten. Sie können aber zu beträchtlichen Schäden führen, weshalb ihre Früher-

30 SR **784.10**

kennung und Abwehr zentral ist. Deshalb muss die Informationsbearbeitung bereits zu einem Zeitpunkt erfolgen, zu dem noch kein rechtsgenügender Verdacht auf die Vorbereitung oder das Vorliegen einer Straftat besteht. Vielmehr muss der NDB aktiv nach diesen Bedrohungen suchen und sie im Verbund mit den anderen Behörden abwehren.

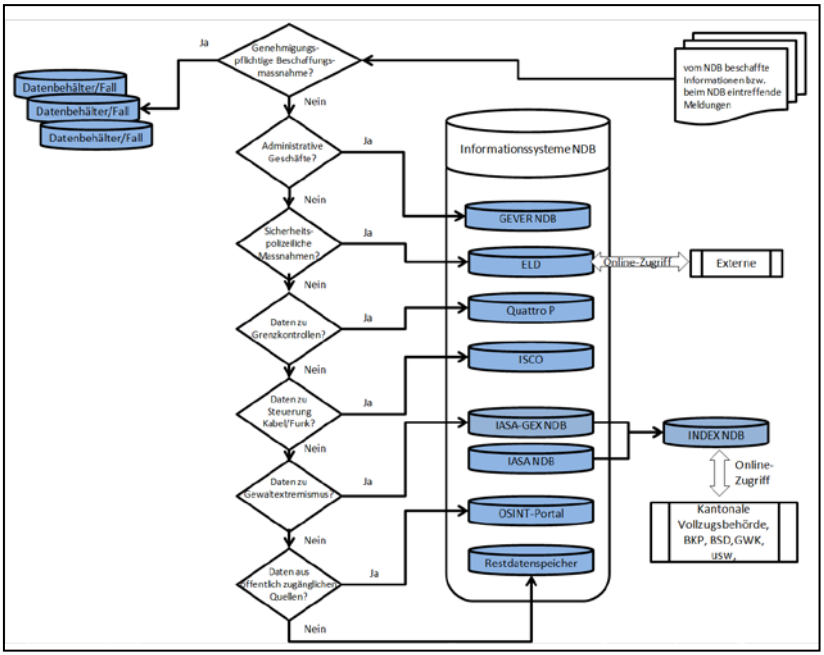
Das vorliegende Gesetz verzichtet konsequent auf die nicht mehr zeitgemässe Trennung zwischen innerer und äusserer Sicherheit, sodass diese Unterscheidung auch bei der Datenbearbeitung durch den NDB keine bestimmende Rolle spielen kann.

Vielmehr ist der fusionierte Nachrichtendienst auf eine einheitliche Regelung der Datenerfassung, -haltung und -bewirtschaftung angewiesen, damit die mit der Fusion angestrebte Effizienzsteigerung und die geforderte gesamtheitliche Auswertung der nachrichtendienstlichen Daten erfolgen kann. Dabei gilt es, die bewährten Punkte aus der langjährigen Praxis mit den bisherigen Rechtsgrundlagen nach dem BWIS und dem ZNDG angemessen zu berücksichtigen.

Der vorliegende Gesetzesentwurf sieht vor, dass die vom NDB beschafften oder bei ihm eintreffenden Meldungen je nach Thematik, Quelle und Sensibilität der Daten in einem Verbund von Informationssystemen abgelegt werden. Der NDB kann nicht wahllos Daten sammeln und aufbewahren. Voraussetzung ist immer ein genügender Bezug zu seinen Aufgaben nach dem NDG. Weiter ist die Einhaltung der Datenbearbeitungsschranke bezüglich der Ausübung der politischen Rechte zu beachten (Art. 5 Abs. 5–8). Schliesslich wird sichergestellt, dass die Daten bereits vor der Ablage auf Erheblichkeit und Richtigkeit überprüft werden. Diese Prüfung erfolgt, bevor Personendaten eine Aussenwirkung entfalten; eine Wirkung entfalten Personendaten, indem sie innerhalb eines Produkts des NDB (z.B. Analysebericht, Meldung an ausländischen Nachrichtendienst, Lagebeurteilung) verwendet werden.

Daten, die der NDB mittels einer genehmigungspflichtigen Beschaffungsmassnahme oder aufgrund von Grenzkontrollen erhält, werden gesondert behandelt und stehen nur den Spezialistinnen und Spezialisten innerhalb des NDB zur Verfügung.

Die verschiedenen Informationssysteme des NDB erlauben eine differenzierte Regelung der Datenhaltung. Während die Datenbearbeitung beispielsweise in den Bereichen Spionageabwehr, Nonproliferation oder Schutz kritischer Infrastrukturen kaum jemals zu Kritik Anlass gab, hat sich die Datenbearbeitung im Bereich des gewalttätigen Extremismus immer wieder als politisch und datenschutzrechtlich besonders sensibel erwiesen. Entsprechend sind für diesen heiklen Bereich strengste Datenbearbeitungsauflagen analog dem BWIS (systematische Qualitätssicherung in kurzen Intervallen) vorgesehen. Die Auflagen bezüglich Meldungen aus öffentlich zugänglichen Quellen sind demgegenüber weniger streng (langsamerer Überprüfungsrhythmus, längere Aufbewahrungsdauer, breiterer Kreis der Zugriffsberechtigten), da solche Daten in der Regel auch aus den Herkunftsquellen weiterhin erschlossen werden könnten, wenn auch anders strukturiert und mit weniger Garantie der Verfügbarkeit.



Art. 43 Grundsätze

Die in Artikel 43 festgehaltenen Grundsätze gelten für alle Informationssysteme des NDB. Dadurch wird, unabhängig davon, in welchem System Personendaten gespeichert sind, ein einheitlich hoher Standard der Datenbearbeitungsqualität sichergestellt. Die Systeme können die Daten in Form von Texten, Ton oder Bild oder anderen geeigneten Formaten enthalten.

Der NDB ist zur Auftragserfüllung immer wieder auf die Bearbeitung besonders schützenswerter Personendaten wie Daten über die Religionszugehörigkeit bei fundamentalistisch motivierten Terroristen, über die Verbüssung von Haftstrafen durch Verurteilte oder über den Gesundheitszustand von Identifikationsfiguren oder ausländischen Politikern angewiesen. Er erstellt und bearbeitet Persönlichkeitsprofile, z.B. zur Einschätzung der Bedrohung durch gewalttätig-extremistische Einzeltä-

ter oder Gruppen. *Absatz 1* schafft für diese Datenbearbeitungen die notwendige formellgesetzliche Grundlage.

In Abweichung zu den üblichen Datenschutzauflagen muss der NDB gemäss *Absatz 2* auch als unrichtig erkannte und entsprechend bewertete Daten aufbewahren dürfen. Bei der Beurteilung von nachrichtendienstlichen Informationen geht es um das Erkennen von Desinformation und Falschinformation. Solche Informationen lassen Absichten von Informationsproduzentinnen und -produzenten wie -lieferantinnen und -lieferanten erkennen. Eine einmal erkannte Desinformation respektive Falschinformation muss auch in Zukunft als solche bekannt und vorhanden sein, um keine späteren Fehlbeurteilungen zu provozieren. Ebenfalls muss bei der internationalen Zusammenarbeit auf identifizierte Falschinformationen zugegriffen werden können, um die spätere Kolportierung von Falschinformationen (z.B. fälschliche Identifikation einer Person als Mitglied einer Terrorgruppe) richtig beurteilen und gegebenenfalls darauf reagieren zu können. Als unrichtig erkannte Daten können darüber hinaus wertvoll sein für die Einschätzung der Zuverlässigkeit, der Vertrauenswürdigkeit oder der Absichten einer menschlichen Quelle oder eines ausländischen Nachrichtendienstes. Die klare Kennzeichnung solcher Daten verhindert, dass sie irrtümlich als richtig weiterbearbeitet werden.

Die Informationssysteme des NDB bilden einen Verbund; sie dienen alle dem Zweck der Erfüllung der gesetzlichen Aufgaben des NDB. Dabei müssen Daten für die Auftragserfüllung oftmals in ein anderes System überführt werden. Die Analytikerin oder der Analytiker, die oder der einen Bericht zu einer terroristischen Gruppierung verfassen muss, ist z.B. auf Meldungen von ausländischen Sicherheitsdiensten, Medienberichten, festgestellten Einreisen in die Schweiz usw. angewiesen. Seine Analysearbeit wird er im dafür vorgesehen Informationssystem IASA NDB nur dann durchführen und belegen können, wenn er die benötigen Daten in IASA NDB zusammengeführt hat. Da dieselben Daten im Ursprungssystem aber auch noch anderen Zwecken dienen können oder von einer umfassenden Meldung oft nur ein Teil für das Erstellen eines bestimmten Produktes benötigt wird, muss die jeweilige Meldung im Originalsystem verbleiben, wo sie anderen Anwenderinnen und Anwendern zur Verfügung steht. Dort wird sie weiterhin regelmässig auf ihre Erheblichkeit und Richtigkeit überprüft (vgl. Art. 44, Qualitätssicherung). Die Daten können somit zwischen den Systemen kopiert werden und unterstehen den jeweiligen Vorgaben der verschiedenen Informationssysteme.

Die schon heute in den Systemen ISIS und ISAS praktizierte Vernetzung von Daten in den Systemen erhöht die Qualität der Ablage und der Auswertemöglichkeiten gegenüber der reinen Ablage von Einzelobjekten. So lassen sich z.B. Beziehungen zwischen Personen untereinander oder mit Ereignissen effizient erfassen und darstellen. Deshalb schafft *Absatz 4* die ausdrückliche Grundlage für solche Vernetzungen und den Einsatz von automatisierten Such- und Auswertungsprogrammen.

Art. 44 Qualitätssicherung

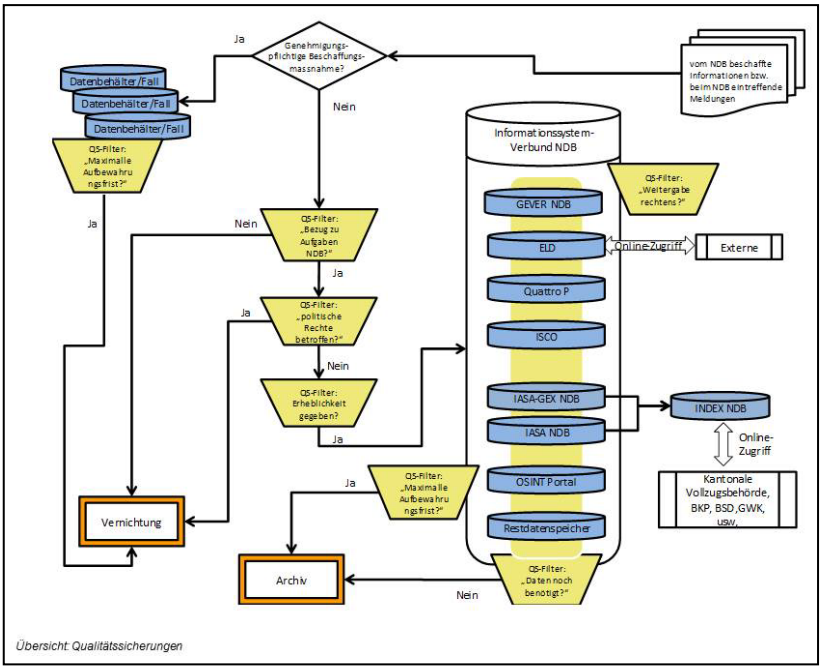
Verschiedene Berichte der Aufsichtsorgane haben aufgezeigt, wie wichtig eine verlässliche und handhabbare Qualitätssicherung für die Güte der Daten des NDB ist. Die Einrichtung einer internen Qualitätssicherungsstelle im NDB hat sich bewährt und soll auch gesetzlich verankert werden. Die Mittel der Qualitätssicherung werden analog zum differenzierten Datenerfassungsmodell gezielt eingesetzt:

- Eine unmittelbare und lückenlose Überprüfung durch die interne Qualitätssicherungsstelle ist bei den Datenbearbeitungen im Bereich des Gewaltextremismus (Abs. 5 Bst. a) sowie bei der Erfassung kantonaler Berichte im INDEX NDB (Abs. 5 Bst. b) sichergestellt. Während in den Bereichen unerlaubter Nachrichtendienst, Proliferation oder Terrorismus zumeist langjährige Entwicklungen zu beobachten sind, ist damit zu rechnen, dass die Qualität der Daten über Gewaltextremismus viel kürzere Halbwertszeiten aufweist. Das Risiko, zwischenzeitlich unnötig gewordene Daten im System zu haben, ist hier bedeutend höher zu veranschlagen und verlangt nach kürzeren Überprüfungszyklen. Für die ebenfalls strikte periodische Überprüfung und periodische Löschung der kantonalen Berichte und ihrer Vorarbeiten sprechen die aktuell strengen Datenbearbeitungsauflagen kantonaler BWIS-Datenbanken. Die Zentralisierung der Datenherrschaft auf Bundesebene soll nicht mit einem Aufweichen dieser Auflagen einhergehen.
- Bei allen übrigen Informationssystemen des NDB sind primär die Benutzerinnen und Benutzer für die regelmässige Durchführung der Qualitätssicherung verantwortlich (Abs. 4). Die interne Qualitätssicherungsstelle sorgt mittels Ausbildung, Vorgaben und Kontrollen für die korrekte Umsetzung der vorgeschriebenen Datenbearbeitungsfilter. Es ist vorgesehen, dass Mitarbeiterinnen und Mitarbeiter nur nach erfolgreich bestandener Prüfung auf die Informationssysteme zugreifen dürfen.
- Zusätzlich führt die Qualitätssicherungsstelle auf allen Systemen Stichproben durch, bei welcher sie die Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit der Datenbearbeitungen überprüft. Diese Kriterien folgen denjenigen der Aufsichtsorgane (Art. 73 ff.). Erkenntnisse daraus fliessen wiederum in die Ausbildung der Benutzerinnen und Benutzer ein.
- Beim System Restdatenspeicher sorgt eine periodische Überprüfung der Meldungen dafür, dass nur Meldungen weiter gespeichert bleiben, die auch den Anforderungen an eine Neuaufnahme genügen würden. Dabei werden nicht sämtliche Personendaten im Detail überprüft, sondern die Erheblichkeit und Richtigkeit eines Informationseingangs als Ganzes (vgl. Art. 56 Abs. 2).

Konkret sorgen folgende Triage-Schritte beim NDB für eine hohe Datenqualität:

- Eingangstriage: Beschränkung auf die Personendaten, die aufgrund des gesetzlichen Auftrags bearbeitet werden können; Beachtung der politischen Rechte; Prüfung aller Daten auf Richtigkeit und Erheblichkeit;
- periodische Überprüfung: die in den Informationssystemen des NDB gespeicherten Personendaten werden regelmässig daraufhin überprüft, ob sie für die Erfüllung der Aufgaben nach diesem Gesetz noch benötigt werden (Erheblichkeitsprüfung). Die Überprüfung umfasst jeweils den gesamten Personendatensatz. Entsprechend werden alle zu einer bestimmten Person oder Organisation erfassten Daten entweder bestätigt oder aber gelöscht. Dies entspricht der bewährten Praxis im ISIS, als auch dem Vorgehen von Partnerdiensten des NDB, sofern diese überhaupt eine periodische Überprüfung der Daten vornehmen;
- Ausgangstriage: nur wenn die Datenbearbeitung rechtens ist, dürfen die Personendaten eine Aussenwirkung entfalten (vgl. Art. 58);

– maximale Aufbewahrungsfristen: der Bundesrat bestimmt für jedes Informationssystem die maximale Aufbewahrungsfrist.



Die *Absätze 1* und *2* definieren die Eingangsbeurteilung, die der NDB vor jeder Erfassung von Daten in ein Informationssystem durchführt.

Massgebend nach *Absatz 1* sind dabei die Erheblichkeit und Richtigkeit der Personendaten. Diese Beurteilung erfolgt für das System Restdatenspeicher, das nicht nach Personenobjekten geordnet ist, nicht für die einzelnen Personendaten einer Meldung, sondern für die Meldung gesamthaft.

Nach *Absatz 2* darf der NDB nur diejenigen Daten bearbeiten, die einen Bezug zu seinen gesetzlichen Aufgaben (Art. 6 Abs. 1) aufweisen. Konkret muss der NDB mit einer Eingangskontrolle bereits vor der Erfassung in ein Informationssystem sicherstellen, dass die erhaltenen Meldungen und Auskünfte einen inhaltlichen Bezug zu gewalttätigem Extremismus, Terrorismus, verbotenem Nachrichtendienst, Proliferation, Angriffen auf kritische Infrastrukturen oder sicherheitspolitisch bedeutsamen

Vorgängen aufweisen. Des Weiteren ist die Bearbeitungsschranke zum Schutz der politischen Rechte (Art. 5 Abs. 5–8) zu beachten.

Vor allem Meldungen der kantonalen Vollzugsbehörden können zur Vervollständigung von Abklärungen an diese retourniert werden, wenn sie für eine Bearbeitung durch den NDB noch nicht genügen. Ist der NDB für die Bearbeitung nicht zuständig, so kann der Absender ein eigenes Interesse oder eine eigene Zuständigkeit haben, eine gemeldete Angelegenheit weiter zu bearbeiten. Auch in solchen Fällen erfolgt eine Rücksendung.

Der NDB sorgt nach *Absatz 4* für eine regelmässige Überprüfung der in allen seinen Informationssystemen gespeicherten Personendaten. Daten, die er nicht mehr für die Erfüllung der Aufgaben benötigt, werden in seinen Systemen gelöscht und nach den Vorgaben des Bundesarchivs archiviert (Art. 67). In der Vernehmlassung war vereinzelt gefordert worden, auf Mehrfacherfassungen (d.h. Erfassung derselben Person in mehreren Systeme) zu verzichten oder solche regelmässig zu überprüfen. Der Bundesrat hält solche Einschränkungen jedoch für nicht zweckmässig, da z.B. eine Mehrfacherfassung in den rein dem NDB vorbehaltenen Systemen und dem System INDEX NDB zwingend ist. Mehrfacherfassungen sind vielmehr aufgrund der Architektur mit mehreren Systemen mit unterschiedlichen Inhalten und Zweckbestimmungen erforderlich und sinnvoll. So sind die Daten immer dort aufzufinden, wo sie aufgrund des Sachzusammenhanges stehen müssen und unterstehen den für das jeweiligen System geltenden Überprüfungs- und Qualitätssicherungsregelungen. Wenn diese eingehalten sind, ist nicht zu erwarten, dass eine zusätzliche Überprüfung der Mehrfacherfassungen zu anderen Beurteilungen führen wird.

Art. 45 Datenbearbeitung in den Kantonen

Absatz 1 liegt folgendes Konzept zugrunde: Soweit die kantonalen Vollzugsbehörden im Anwendungsbereich dieser Vorlage tätig sind, arbeiten sie ausschliesslich mit Informationssystemen, die ihnen der Bund zur Verfügung stellt. So erlaubt z.B. der INDEX NDB den Kantonen die Erfassung von Vorabklärungen zu Berichten an den Bund, die Auftragsverwaltung und die Ablage ihrer Berichte (vgl. Art. 50). Die Daten werden ausschliesslich vom Bund bzw. vom NDB verwaltet und unterstehen dem Datenschutzrecht des Bundes. Im Anwendungsbereich dieser Vorlage ist der Bund der alleinige Datenherr.

Die Daten nach *Absatz 2* bearbeiten die Kantone entweder im Rahmen der eigenen, kantonalen nachrichtendienstlichen Tätigkeit (ausserhalb der Zuständigkeit des Bundes bzw. des NDB) oder bei der Wahrnehmung anderer sicherheits- oder kriminalpolizeilicher Aufgaben. So bearbeiten die Kantone beispielsweise die Daten zu Bewilligungsgesuchen für Kundgebungen in eigener Kompetenz. Sind dabei gewalttätig-extremistische Ausschreitungen zu befürchten, so bearbeitet sie der NDB auch unter diesem Gesichtspunkt. Verläuft die Kundgebung tatsächlich gewalttätig, so bearbeitet der NDB diese Informationen unter dem Gesichtspunkt des gewalttätigen Extremismus nach diesem Gesetz, während die kantonalen Behörden die Straftaten wie Sachbeschädigung, Landfriedensbruch oder Körperverletzung in eigener Kompetenz bearbeiten. Wegen der unterschiedlichen Auskunftsregelungen für diese Datenbearbeitungen ist zu vermeiden, dass der eine Datenbestand Hinweise auf den anderen enthält. Die Vollzugsvorschriften können Ausnahmen vorsehen, z.B. wenn Meldungen gar keine Personendaten enthalten oder wenn den betroffenen Personen

die beidseitige Bearbeitung bekannt ist, z.B. aufgrund von entsprechenden Vorhalten bei Befragungen.

Aufgrund der Vernehmlassung wurde Absatz 3 ergänzt, der die Verwendung von Erkenntnissen der Lagebeurteilungen innerhalb der Kantone ermöglicht; dies ist schon heute unter den Regelungen des BWIS möglich. Ebenfalls ergänzt und präzisiert wurden Bestimmungen über die Datenhaltung der Kantone (Art. 50) und deren kantonale Kontrolle und Aufsicht (Art. 78).

Art. 46 Informationssysteme des NDB

Artikel 46 definiert den Verbund von Informationssystemen, den der NDB zur Erfüllung seiner Aufgaben betreibt. Der Verbund ist vergleichbar mit dem Verbund der polizeilichen Informationssysteme, wie er im Bundesgesetz vom 13. Juni 2008[31] über die polizeilichen Informationssysteme des Bundes (BPI) geregelt ist (vgl. Art. 2 BPI).

Der Artikel erlaubt den Überblick über alle Informationssysteme des NDB, die ihre formellgesetzliche Grundlage in der Vorlage finden. Jedes Informationssystem wird nachfolgend in einem eigenen Artikel behandelt.

Der Bundesrat erhält in *Absatz 2* den Auftrag, für jedes Informationssystem die Einzelheiten der Datenbearbeitung festzulegen. Darunter fallen insbesondere auch die Fristen für die periodischen Überprüfungen und die maximale Aufbewahrungsdauer. Die Delegation dieser Detailregelungen an den Bundesrat entspricht der heutigen Regelung und dem üblichen Vorgehen bei Informationssystemen. Die Verordnung vom 4. Dezember 2009[32] über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB) legt heute beispielsweise die maximalen Aufbewahrungsfristen fest. Diese liegt bei den Daten über die Auslandsaufklärung bei 30 Jahren nach der letzten Bearbeitung, höchstens aber bei 45 Jahren. Bei den Inlanddaten beträgt sie je nach Herkunft der Daten zwischen fünf Jahren (Daten aus Personensicherheitsprüfungen) und 45 Jahren (Daten aus öffentlich zugänglichen Quellen). Ebenso legt die ISV-NDB die periodischen Überprüfungsfristen der Daten der Inlandaufklärung auf fünf Jahre nach der ersten Erfassung fest; danach werden die Daten alle drei Jahre einer wiederkehrenden Überprüfung unterzogen, bis die maximale Aufbewahrungsdauer erreicht worden ist. Das NDG legt hierfür fest, dass der Bundesrat bei der Festlegung dieser Fristen die besonderen Eigenschaften der Daten bzw. der Bedürfnisse der Aufgabengebiete berücksichtigen muss. Damit sollen wie bisher differenzierte Lösungen für die verschiedenen Systeme und Datenkategorien getroffen werden.

Die Ausführungsbestimmungen werden ferner detaillierte Regelungen enthalten, welche Zugriffsberechtige zu welchen Datenbearbeitungen (wie Lesen, Schreiben, Ändern, Löschen) berechtigt sind, wer und wie systemübergreifende Datenabfragen ausführen kann und welche Behörden des Bundes und der Kantone aus den Bereichen Polizei, Justiz und Strafverfolgung ausserhalb des NDB auf den INDEX NDB zugreifen können.

31 SR **361**
32 SR **121.2**

Im weiteren wird der NDB gemäss den allgemeinen datenschutz- und informationsschutzrechtlichen Vorgaben zu allen Informationssystemen Bearbeitungsreglemente erlassen, welche insbesondere die interne Organisation sowie das Datenbearbeitungs- und Kontrollverfahren umschreiben und die Unterlagen über die Planung, die Realisierung und den Betrieb der Datensammlung und der Informatikmittel enthalten.

Art. 47 Zuweisung der Daten zu den Informationssystemen

Die beim NDB eingehenden Daten werden in einem ersten Schritt auf die Erheblichkeit für die Aufgabenerfüllung und ihre Richtigkeit beurteilt. Danach weist sie die zuständige Stelle des NDB dem für die jeweilige Datenart vorgesehenen System zu. Den Systemen IASA NDB und INDEX NDB werden keine Daten direkt zugewiesen. IASA dient den Auswerterinnen und Auswertern des NDB dazu, die für die Produktion notwendigen Daten und Erkenntnisse zusammenzutragen, auszuwerten und zu dokumentieren. Der INDEX NDB enthält von Seiten des NDB vor allem die Identifikationsdaten für Personen, Organisationen, Gegenstände und Ereignisse, die aus den Systemen IASA NDB und IASA-GEX NDB in den INDEX NDB kopiert werden.

Art. 48 IASA NDB

Artikel 48 bildet die formellgesetzliche Grundlage für das Integrale Analysesystem des NDB (IASA NDB), das System zur nachrichtendienstlichen Auswertung für alle Aufgabengebiete des NDB mit Ausnahme des gewalttätigen Extremismus. Diese Daten dürfen nach dem neuen System ausschliesslich im System IASA-GEX NDB bearbeitet werden (Art. 49). IASA NDB löst damit weitestgehend das heutige Informationssystem innere Sicherheit (ISIS) und das Informationssystem äussere Sicherheit (ISAS) ab.

Diejenigen Fachbereiche, die für das Erfassen verantwortlich sind, führen in ihrem Spezialgebiet die periodischen Überprüfungen der im IASA NDB gespeicherten Daten durch. Die interne Qualitätssicherungsstelle führt zusätzlich regelmässig Stichproben durch, um die gesetzeskonforme Bearbeitung zu kontrollieren (vgl. Art. 44).

Art. 49 IASA-GEX NDB

Daten über gewalttätigen Extremismus haben oft stärkere ausschliessliche Bezüge zur Schweiz als Daten anderer Arbeitsgebiete des NDB. Sie sind oft auch heikler, da hier die Nähe zur grundrechtlich geschützten und in Artikel 5 Absatz 5 NDG der Informationsbeschaffung und -bearbeitung entzogenen politischen Betätigung grösser ist. Sie werden deshalb im besonderen Informationssystem Integrales Analysesystem Gewaltextremismus des NDB (IASA-GEX NDB) erfasst, das der zentralen Erfassung, Bearbeitung und Auswertung aller Daten im Bereich des Gewaltextremismus dient. Dort unterstehen sie auch der strengeren und regelmässigeren Überprüfung durch die interne Qualitätssicherungsstelle des NDB (Art. 44 Abs. 5 Bst. a).

Der Bundesrat legt gemäss Artikel 69 Absatz 1 Buchstabe c jährlich fest, welche Gruppierungen, als gewalttätig-extremistisch einzustufen sind.

Art. 50 INDEX NDB

Der INDEX NDB dient einerseits dazu, festzustellen, ob der NDB Daten zu einer bestimmten Person, Organisation, einem Gegenstand oder einem Ereignis bearbeitet. Alle in IASA NDB und IASA-GEX NDB erfassten Personen sind hier abrufbar. Konkret werden hier die wichtigsten Identifikationsdaten erfasst, beispielsweise bei Personen der Name, das Geburtsdatum, die Nationalität usw. Auf den Index haben auch die berechtigten Stellen Zugriff, welche nicht am besonders gesicherten Netzwerk des NDB angeschlossen sind.

Der INDEX NDB dient damit der Koordination der nachrichtendienstlichen Tätigkeiten von Bund und Kantonen, aber auch der Koordination von nachrichtendienstlichen Tätigkeiten mit sicherheits- und kriminalpolizeilichen Tätigkeiten. Heute erfolgt dies, indem Amtsstellen ausserhalb des NDB einen auf die Identifikationsdaten eingeschränkten direkten Zugriff auf ISIS haben. Stellen ausserhalb des NDB und der kantonalen Vollzugsbehörden haben keinen Zugang zu Informationen, die über die Identifikationsdaten hinausgehen. Sie müssen mit dem NDB in Kontakt treten, um allenfalls weitere Daten auf dem Weg der formellen Zusammenarbeit und Datenweitergabe (Art. 58 ff.) zu erhalten.

Der INDEX NDB ist als besonderes System für diesen Zweck notwendig, da IASA NDB und IASA-GEX NDB aus Sicherheitsgründen im besonders geschützten Netzwerk des NDB betrieben werden sollen, das keine Zugriffe von Stellen ausserhalb des NDB erlaubt. Der INDEX NDB ermöglicht die rasche Abfrage der Identifikationsdaten für die berechtigten Drittstellen, während die vollständigen Daten des NDB vor Zugriffen von aussen geschützt bleiben.

Andererseits dient der INDEX NDB als Plattform für die Datenbearbeitung durch die kantonalen Vollzugsbehörden. Diese bearbeiten in diesem System die Daten, bevor sie dem NDB Bericht erstatten. Der Index erlaubt ihnen weiter die Übersicht über die Aufträge des Bundes und die Ablage. Mit dieser Zentralisierung aller Datenbearbeitungen, die im Rahmen dieser Vorlage erfolgen, wird auf Bundesebene eine einheitliche Regelung und Kontrolle sichergestellt.

In der Vernehmlassung hatten einige Kantone den Wunsch geäussert, dass die Kantone gegenseitig Zugriff auf ihre kantonalen Daten nehmen können. Bei der Abklärung dieses Wunsches wurde erkannt, dass eher das Bedürfnis nach einer sicheren Übermittlung von Daten unter den Kantonen besteht. Dieses Anliegen wurde deshalb neu in Absatz 2 aufgenommen.

Art. 51 GEVER NDB

Bei GEVER NDB handelt es sich um eine Standardgeschäftsverwaltung, wie sie in anderen Bereichen der Bundesverwaltung auch in Betrieb ist. Der NDB bearbeitet jedoch typischerweise vor allem nachrichtendienstliche Geschäfte, wie Analyseberichte, schriftliche oder mündlich vorzutragende Lageeinschätzungen oder Antworten auf Einzelanfragen. Diese werden wie rein administrative Geschäfte (z.B. Stellungnahmen zu Ämterkonsultationen, Finanzabläufe, Personalgeschäfte usw.) in diesem zentralen System verwaltet, das so einen Überblick und die Geschäftskontrolle über alle laufenden und abgeschlossenen Geschäfte erlaubt. Über den mit dem Bundesarchiv abgestimmten Aktenplan wird über GEVER NDB die Archivierung der Produkte des NDB sichergestellt.

Zum Schutz der nachrichtendienstlichen Daten betreibt der NDB GEVER NDB ebenfalls in seinem besonders geschützten Netzwerk, das heisst es gibt keine Zugriffe von Drittstellen.

Art. 52 ELD

Artikel 52 übernimmt von Artikel 10*a* BWIS die formellgesetzliche Grundlage für die ELD, das System für die elektronische Lagedarstellung des NDB. Die Regelung entspricht weitgehend der am 16. Juli 2012 in Kraft getretenen Revision des BWIS.

Personendaten werden in der ELD nur insofern geführt, als dies zur Lagedarstellung und -beurteilung unbedingt notwendig ist.

Der Zugang von Privaten oder ausländischen Behörden auf die ELD hat im Rahmen von BWIS II zu erheblichen Diskussionen geführt. Die bisherige Praxis hat die restriktive Anwendung dieser Bestimmung durch den NDB bestätigt. Der Bundesrat ist aber nach wie vor überzeugt, dass die Schweiz als Gastgeberin internationaler Veranstaltungen im Verbund mit privaten und ausländischen Partnern für die Sicherheit sorgen muss. Erfahrungen wie z.B. mit der EURO 08 haben gezeigt, dass es bei grösseren Veranstaltungen mit erhöhtem Gefährdungspotenzial notwendig sein kann, auch privaten Organisationen oder ausländischen Partnern unverzüglich Zugriff auf bestimmte Daten der ELD NDB zu geben. Dabei ist jeweils der Grundsatz der Verhältnismässigkeit zu wahren, das heisst der NDB ermöglicht den Zugriff nur auf die Daten, die für diese besondere Bedrohungsabwehr benötigt werden.

Art. 53 OSINT-Portal

Artikel 53 bildet die formellgesetzliche Grundlage für das OSINT-Portal, das System des NDB zur Nutzung der öffentlich zugänglichen Daten. Eine Speicherung z.B. von Internetdaten ist für die zielgerichtete Auswertung unerlässlich, da sonst bei jeder neuen Recherche jeweils wieder im gesamten Internet gesucht werden müsste und zudem im Internet die Verfügbarkeit von früher vorhandenen Daten nicht gesichert ist.

Da es sich um Daten handelt, die grundsätzlich jedermann zugänglich sind, sollen sie auch innerhalb des NDB weniger restriktiv behandelt werden als Daten aus anderen Quellen. Somit ist es auch nicht sinnvoll, in *Absatz 3* den Zugriff innerhalb des NDB einzuschränken.

Auf Wunsch der Kantone in der Vernehmlassung wurde Absatz 4 ergänzt, der den kantonalen Vollzugsbehörden den Zugriff auf Teile des OSINT-Portals ermöglicht. Ein vollständiger Zugriff wäre unter anderem aus urheberrechtlichen Gründen nicht zulässig.

Art. 54 Quattro P

Der NDB lässt von den Grenzkontrollorganen an den schweizerischen Flughäfen schon heute Einreisedaten von bestimmten Personen aus bestimmten Herkunftsländern zum Zweck der Früherkennung von Spionage und Proliferation erfassen. Diese Daten soll er auf einem separaten Informationssystem mit dem Namen Quattro P bearbeiten («Programme préventif de contrôle des passeports», bisher im Informatikmodul P4 nach Art. 25 Abs. 1 Bst. h ISV-NDB). Die Formulierungen dieses

Artikels im Vernehmlassungsentwurf führten zu einigen Missverständnissen, weshalb er neu präziser gefasst ist.

Zugriff hat nach *Absatz 3* nur ein kleiner Personenkreis innerhalb des NDB, der mit der Erfassung, Recherche und Auswertung dieser Daten beauftragt ist (heute weniger als zehn Personen). Aus diesem Grund ist auch weiterhin kein Zugriff für die Kantone vorgesehen.

Der Bundesrat bestimmt nach *Absatz 4* jährlich den Umfang der Kategorien der zu erfassenden Personen, das heisst die massgebenden Herkunftsländer und allfällige Einschränkungen auf bestimmte Personenkategorien (z.B. nur Männer oder nur Inhaber/innen von bestimmten Arten von Pässen). Das Vorgehen ist vergleichbar mit demjenigen nach Artikel 20 Absatz 4, wonach der Bundesrat festlegt, welche Vorgänge und Feststellungen dem NDB unaufgefordert zu melden sind. Für die Daten des Systems Quattro P gilt heute eine maximale Aufbewahrungsdauer von fünf Jahren (Art. 33 Abs. 1 Bst. i ISV-NDB).

Art. 55 ISCO

Das Informationssystem COMINT (ISCO) dient dem NDB zur Verwaltung und Steuerung seiner Aufträge an das ZEO. Die Steuerung der Funk- und Kabelaufklärung geschieht durch schriftliche Aufträge des NDB (vgl. Art. 37). In diesen werden der Aufklärungsauftrag, die Informationen zu den konkreten Aufklärungsobjekten, die erwarteten Resultate sowie weitere Rahmenbedingungen für die Auftragsabwicklung festgehalten. Ebenfalls Teil von ISCO sind die Resultate der NDB-internen periodischen Überprüfungen der Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit der Aufklärungsmassnahmen. Die Daten von ISCO dienen den Aufsichtsorganen (insbesondere der UKI, vgl. Art. 75) als Basis für ihre Tätigkeiten.

Zugriff auf ISCO haben nur sehr wenige Mitarbeiterinnen und Mitarbeiter des NDB, die mit der unmittelbaren Steuerung der Aufträge befasst sind (heute weniger als zehn Personen).

Die Erfassung der Resultate der Funk- und Kabelaufklärung zur weiteren Auswertung und Verwendung in Produkten, Lagefortschreibungen usw. erfolgt im Restdatenspeicher (Art. 56).

Art. 56 Restdatenspeicher

Im Restdatenspeicher werden alle Informationen abgespeichert, die bei der Triage nach der Eingangsprüfung nicht einem anderen System zugewiesen werden konnten. Es handelt sich dabei vor allem um die Meldungen von ausländischen Sicherheitsbehörden, Daten aus der Funk- und Kabelaufklärung, Informationen von menschlichen Quellen und nicht aktiv vom NDB beschaffte Informationen. Der Restdatenspeicher enthält keine Daten zum gewalttätigen Extremismus – diese werden alle im System IASA-GEX NDB erfasst und bearbeitet.

Informationen aus dem Restdatenspeicher werden vor allem zu Analysezwecken in das System IASA übertragen, wenn sie für das Erstellen von nachrichtendienstlichen Produkten oder für Lagefortschreibungen, Studien oder Ähnliches benötigt werden.

Mit periodischen Kontrollen stellt der NDB sicher, dass der Restdatenspeicher nur Informationen enthält, die jeweils den aktuellen Erfassungskriterien der Erheblichkeit (Bezug zu einem Aufgabengebiet des NDB, Beachtung von Art. 5 Abs. 5–8

NDG) und Richtigkeit entsprechen. Andernfalls werden die Daten gelöscht bzw. notwendige unrichtige Informationen als unrichtig bezeichnet. Wie bei der Eingangsprüfung erfolgt die periodische Beurteilung anhand der gesamten Meldung, das heisst es werden keine Einzelaussagen eines grösseren Dokuments wie z.B. einer Personenliste überprüft.

Art. 57 Daten aus genehmigungspflichtigen Beschaffungsmassnahmen

Daten, die durch genehmigungspflichtige Beschaffungsmassnahmen unter Einsatz technologischer Mittel (wie z.B. bei einer Kommunikationsüberwachung) beschafft werden, können zum einen sehr umfangreich sein und zum anderen viele Informationen enthalten, die nichts mit dem Aufklärungsziel zu tun haben, weil sie z.B. rein privater Natur sind. Auch dem Persönlichkeitsschutz Dritter, die z.B. den Fernmeldeanschluss der überwachten Person benutzen, ist Rechnung zu tragen. Oft lässt sich nicht auf Anhieb feststellen, ob bestimmte Kommunikationen relevant sind oder nicht, weil beispielsweise das Kontaktnetz der überwachten Person erst noch identifiziert werden muss oder weil diese zum Schutz ihrer Kontakte konspirative Elemente in der Kommunikation anwendet. Informationen können deshalb nicht sofort als notwendig oder nicht notwendig identifiziert werden.

Nicht zuletzt dient die Speicherung in separaten Systemen auch dem Schutz der Informatikinfrastruktur des NDB, da z.B. bei der Überwachung von Internetkommunikationen oder beim Eindringen in Computersysteme auch Schadsoftware (Viren, Trojaner) auftauchen können. Diese sollten nicht in die Systeme des NDB eingeschleppt werden.

Artikel 57 sieht deshalb vor, dass Daten aus solchen Beschaffungsmassnahmen in vom Verbund von Informationssystemen getrennten Systemen gespeichert und dort gesichtet werden. Nur für die Zwecke des Auftrags notwendige Daten übernimmt der NDB nach *Absatz 2* zur weiteren Auswertung in die entsprechenden Informationssysteme des Verbunds, in der Regel in das IASA NDB.

Für Daten der Auslandbeschaffung, die mit vergleichbaren Massnahmen beschafft wurden, regelt Artikel 35 Absatz 5 eine analoge Möglichkeit der separaten Speicherung.

Entsprechend schränkt *Absatz 3* den Zugriff auf diese Daten auf diejenigen Personen ein, welche mit der unmittelbaren Durchführung der Massnahme und der Auswertung ihrer Ergebnisse beauftragt sind. Dies werden in der Regel die zuständigen Sachbearbeiterinnen und Sachbearbeiter der Beschaffung und Auswertung sein, die den jeweiligen Fall bearbeiten.

Die in Frage kommenden Speicher werden in der Regel Computersysteme sein, die nicht mit dem gesicherten Netzwerk des NDB verbunden sind. Der Bundesrat regelt auch für diese in der Verordnung die üblichen Details (Datensatz, Bearbeitungs- und Zugriffsrechte usw.).

Art. 58 Überprüfung vor der Weitergabe

Nicht nur die mit der Qualitätssicherung beauftragten Stellen des NDB, sondern jede an einer Weiterleitung von Informationen des NDB beteiligte Person ist verpflichtet, die Qualität der Daten vor einer Weitergabe zu beurteilen. Sie ist verpflichtet, sicherzustellen, dass die rechtlichen Voraussetzungen für die Weiterleitung erfüllt sind und die Personendaten korrekt bearbeitet werden.

Art. 59 Weitergabe von Personendaten an inländische Behörden

Damit der NDB seinen Auftrag zur Frühwarnung und Prävention erfüllen kann, muss er Personendaten an politische Behörden, Strafverfolgungs-, Justiz- und Sicherheitsbehörden weiterleiten können. Die Regelung entspricht weitgehend geltendem Recht (Art. 17 BWIS), wurde im NDG aber noch weiter ausgebaut und differenziert.

Namentlich die Weitergabe von Daten aus genehmigungspflichtigen Beschaffungsmassnahmen erfordert weitere Schutzmassnahmen. Damit soll verhindert werden, dass z.B. bei Fernmeldeüberwachungen festgestellte, geringfügige Straftaten den Strafverfolgungsbehörden gemeldet werden. Das Strafprozessrecht enthält eine vergleichbare Regelung für solche sogenannten Zufallsfunde (Art. 278 StPO). Das NDG übernimmt deshalb in *Absatz 3* den Grundsatz, dass nur Erkenntnisse bezüglich Straftaten verwendet werden dürfen, für deren Verfolgung auch die vergleichbare strafprozessrechtliche Überwachungsmassnahme hätte angeordnet werden dürfen. Eine weitere Angleichung an das Strafprozessrecht ist indessen nicht sinnvoll, da das NDG primär anderen Zwecken dient als die Strafverfolgung und zudem auch andere Verwaltungsbereiche verpflichtet sind, bei ihnen vorliegende Informationen über Straftaten an die Strafverfolgungsbehörden weiterzuleiten.

In der Vernehmlassung waren hier sich zum Teil widersprechende Forderungen nach mehr oder weniger Datenweiterleitungen an die Strafverfolgungsbehörden gestellt worden. Mit der hier diskutierten Vorlage wird nach Auffassung des Bundesrats eine ausgewogene Lösung vorgeschlagen.

Art. 60 Weitergabe von Personendaten an ausländische Behörden

Dieser Artikel übernimmt weitgehend die Bestimmungen von Artikel 17 BWIS. Das Datenschutzrecht sieht in der Regel vor, dass Personendaten nur an Staaten weitergegeben werden dürfen, die einen mit dem schweizerischen Niveau vergleichbaren Datenschutz garantieren (Art. 6 Abs. 1 DSG). Mit dieser Bestimmung würden die meisten aussereuropäischen Länder von der Zusammenarbeit mit dem NDB ausgeschlossen, falls nicht im Einzelfall die restriktiven Ausnahmen von Artikel 6 Absatz 2 DSG zur Anwendung kommen könnten. Dieser Ausschluss würde den NDB von wichtigen Informationsquellen gerade in Krisenregionen ausschliessen.

Schon das BWIS stellt deshalb besondere Regelungen für die nachrichtendienstliche Zusammenarbeit mit dem Ausland und die Weitergabe von Personendaten auf, die das NDG hier übernimmt. Dazu besteht eine lange und von den Aufsichtsorganen (ND-Aufsicht des VBS und früher des EJPD und Geschäftsprüfungsdelegation der eidgenössischen Räte) begleitete und kontrollierte Praxis.

Die Zusammenarbeit und der Datenaustausch mit ausländischen Sicherheitsbehörden, die nicht Nachrichtendienste im engeren Sinn sind, beschränkt sich dabei auf deren Funktionen, die mit den Aufgaben des NDB vergleichbar sind. Die Zusammenarbeit anderer schweizerischer Dienststellen in ihren Zuständigkeitsbereichen mit ausländischen Sicherheitsbehörden wird dadurch nicht eingeschränkt, und für die Weitergabe ihrer Daten sind diese nach ihren Rechtsgrundlagen zuständig.

Absatz 2 Buchstabe d betrifft die schon in Artikel 12 Absatz 1 Buchstabe d erwähnten Unbedenklichkeitsanfragen oder Clearings zugunsten von (in der Regel Schweizer) Personen, die im Ausland Zugang zu klassifizierten Projekten, Informationen, Anlagen usw. erhalten sollen. Solche Auskünfte sind in der Regel im Interesse der

betroffenen Person, die sonst eine Arbeitsstelle oder eine geschäftliche Tätigkeit nicht antreten könnte.

Art. 61 Weitergabe von Personendaten an Dritte

Die nachrichtendienstliche Tätigkeit macht es bisweilen erforderlich, auch Daten an private Dritte weiterzugeben. Häufigster Anwendungsfall ist dabei das Begründen eines eigenen Auskunftsgesuchs. Beim Einholen von Auskünften über natürliche oder juristische Personen muss der NDB gegenüber der befragten Person natürlich sagen können, über welche Person und in welchem Zusammenhang er eine Auskunft braucht. Die Bestimmung entspricht dem heutigen Artikel 17 Absatz 3 BWIS.

Art. 62–65 Auskunftsrecht

Für das Auskunftsrecht übernimmt der Entwurf inhaltlich weitgehend die vom Parlament im Rahmen «BWIS II reduziert» beschlossene Lösung, die sich an das BPI anlehnt. Im Gegensatz zum am 16. Juli 2012 in Kraft getretenen Artikel 18 BWIS ist hier die Regelung indessen in mehrere Artikel gegliedert, was ihre Lesbarkeit und Verständlichkeit erhöht.

Das alte indirekte Auskunftsrecht nach dem BWIS war vom Bundesgericht, sofern mit einer wirksamen Beschwerdemöglichkeit ausgestattet, als verfassungskonform beurteilt worden. Die ursprüngliche Vorlage BWIS II enthielt deshalb eine solche Lösung, die aber zurückgewiesen wurde. Der Bundesrat beantragte in der Folge, das DSG auch im BWIS integral anzuwenden. Das Parlament entschied sich jedoch bewusst für die Lösung analog dem BPI. Der Bundesrat hält auch heute noch andere Lösungen für machbar, erachtet es aber nicht als sinnvoll, dem Parlament im NDG erneut eine andere Auskunftsregelung zu unterbreiten.

Der Ablauf sieht vor, dass der NDB zuerst eine Auskunftserteilung prüft, im Falle von Geheimhaltungsinteressen oder bei nicht verzeichneten Personen jedoch die Auskunft aufschiebt. Die betroffene Person kann danach an den EDÖB gelangen, der sinngemäss das frühere Verfahren der indirekten Auskunft durchführt.

Als Abweichung zur aktuellen BWIS-Regelung schlägt der Bundesrat vor, in Artikel 63 Absatz 5 auf die ursprüngliche Formulierung im BPI zurückzukommen. Das BPI sieht hier vor, dass ausnahmsweise bei einem Aufschub der Auskunft (wegen Geheimhaltungsinteressen oder bei nicht verzeichneten Personen) auf Empfehlung des EDÖB Auskunft erteilt werden kann, wenn damit keine Gefährdung der inneren oder der äusseren Sicherheit verbunden ist und eine Person glaubhaft darlegen kann, dass ihr bei einem Aufschub der Auskunft ein erheblicher, nicht wiedergutzumachender Schaden erwachsen würde.

Im BWIS wurde hier gegenüber dem BPI die Beweislast umgekehrt, indem der NDB auf Empfehlung des EDÖB Auskunft erteilen soll, wenn und soweit damit keine Gefährdung der inneren oder äusseren Sicherheit verbunden ist. Bei nicht verzeichneten Personen kann der NDB diesen Nachweis jedoch kaum einmal erbringen, weil ihm über diese Personen gerade keine Informationen vorliegen. Damit würde die Regel von Artikel 62 Absatz 2 Buchstabe c ausgehebelt, welche besagt, dass bei nicht verzeichneten Personen die Auskunft aufgeschoben wird. Deshalb wird bei der hier diskutierten Vorlage das Vorgehen gemäss BPI als sachlich richtiger erachtet.

Art. 66 Ausnahme vom Öffentlichkeitsprinzip

Die Erfahrungen, die der NDB seit seinem Bestehen mit Einsichtsbegehren gestützt auf das BGÖ gemacht hat, haben aufgezeigt, dass der besondere Schutzbedarf der nachrichtendienstlichen Informationen nur schwer mit dem Transparenzgedanken des BGÖ vereinbar ist.

Die bisherigen Zugangsgesuche betrafen jeweils vorwiegend Dokumente und Dossiers über die Beschaffung von Informationen durch den NDB oder über Aktionen, die der NDB (oder seine Vorgänger) durchgeführt hatte. Vereinzelt wurde auch ausdrücklich Einsicht in andere Unterlagen, z.B. über den Verkehr mit ausländischen Nachrichtendiensten und Sicherheitsbehörden, verlangt. Mit Rücksicht auf die beteiligten Personen oder ausländischen Dienste und im Einklang mit den Ausnahmeregelungen des BGÖ muss der NDB die Einsicht in Beschaffungs- und Zusammenarbeitsdossiers nach ausführlicher Prüfung und interner Begründung jeweils ablehnen. Es ist deshalb nicht sinnvoll, hier den Grundsatz aufrecht zu erhalten, dass in Dokumente über die nachrichtendienstliche Beschaffung Einsicht gegeben werden muss, wenn von vornherein feststeht, dass diese den Ausnahmebestimmungen des BGÖ unterstehen.

Geprüft wurde, ob eine vollständige Ausnahme des NDB aus dem Geltungsbereich des BGÖ notwendig sei. Da aber der NDB auch reine Verwaltungsgeschäfte betreut, für welche die Auskunft nach dem BGÖ durchaus möglich ist, schlägt der Bundesrat nur eine sachliche Ausnahme für die Unterlagen über die nachrichtendienstliche Informationsbeschaffung vor.

Art. 67 Archivierung

Die Daten und Akten des NDB unterstehen grundsätzlich dem Archivierungsgesetz vom 26. Juni 1998[33]. Dieses sieht die lückenlose Archivierung aller vom Bundesarchiv als archivwürdig befundenen Akten vor. Auf der anderen Seite befinden sich in den Akten des Nachrichtendienstes auch Akten, die von ausländischen Partnerdiensten stammen und die nur unter dem Vorbehalt des Quellenschutzes zugestellt wurden. Wird ein solcher Schutz nicht mehr gewährleistet, versiegen die Informationen, die Schweiz wäre bei der Bekämpfung von globalen Bedrohungen wie Terror, Nonproliferation, gewalttätigem Extremismus und Spionage isoliert.

Der Artikel nimmt in den *Absätzen 1 und 2* beide Interessen auf, diejenige des Bundesarchivs an einer möglichst lückenlosen Archivierung, aber auch das berechtigte Interesse der Sicherheitsbehörden an einem effektiven Quellenschutz. Die Daten und Akten des NDB werden durch das Bundesarchiv in besonders gesicherten Räumen vollständig archiviert. Bei einem konkreten Einsichtsgesuch kann die Einsichtnahme im Einzelfall schon in Anwendung der Bestimmungen des Archivierungsgesetzes beschränkt oder untersagt werden, wenn ein überwiegendes schutzwürdiges öffentliches oder privates Interesse gegen die Einsichtnahme besteht. Ein entgegenstehendes öffentliches Interesse besteht, wenn der betroffene ausländische Dienst der Einsichtnahme begründet nicht zustimmt, was Absatz 2 verdeutlicht. Der NDB wird das betroffene Archivgut bei der Ablieferung entsprechend kennzeichnen, damit das Bundesarchiv leicht identifizieren kann, in welchen Fällen es eine Rücksprache mit dem NDB nehmen muss. Andere Länder wenden dieses Vorgehen gegenüber der Schweiz ebenfalls an.

33 SR **152.1**

In Einzelfällen muss der NDB Einsicht in archivierte Personendaten nehmen können (*Abs. 3*). Analoge Regelungen gibt es bereits heute für Strafverfolgungsbehörden. Beispiel: Der NDB erhält von einem ausländischen Nachrichtendienst eine Anfrage im Zusammenhang mit wiederaufgenommen Abklärungen zu einem Terroranschlag. Der NDB hat die Daten zu seinen damaligen Erkenntnissen in der Schweiz aber bereits gelöscht und dem Bundesarchiv abgeliefert.

Art. 68 Dienstleistungen

Der NDB ist grundsätzlich wie jede andere Amtsstelle berechtigt und verpflichtet, Amtshilfe in den Bereichen zu leisten, wo er sowohl zuständig als auch personell und fachlich dazu in der Lage ist. Der NDB kann hier besondere operative Mittel und Methoden zur Verfügung stellen, beispielsweise Übermittlungs-, Transport- und Beratungsleistungen, über die andere Amtsstellen nicht verfügen.

So kommen regelmässig gesicherte Kommunikationsmittel des NDB im Rahmen des internationalen Krisenmanagements (z.B. bei Entführungsfällen) zum Einsatz, namentlich chiffrierte Mobiltelefone. Die Sicherheitsorgane des Bundes und internationaler Organisationen greifen auf die Kompetenzen des NDB im Bereich Abhörsicherheit und Informationsschutz zurück, z.B. beim Durchsuchen von Räumen auf Abhöreinrichtungen. Der NDB berät die zuständigen Stellen des Bundes bei Beschaffungen von Tresoren und spezieller Schliesstechnik. Ausländische Nachrichtendienste und Sicherheitsbehörden werden vom NDB unter anderem durch Spezialtransporte unterstützt.

In einem erfolgreich zu Ende gegangenen Entführungsfall unterstützte der NDB im Rahmen des Krisenmanagements mit folgenden Dienstleistungen:

- Er stellte gesicherte Kommunikationsmittel für die Verbindung des Krisenmanagement-Zentrums des EDA mit der lokalen Vertretung des EDA zur Verfügung und leistete den technischen Support.
- Er stellte seine sicheren Kommunikationsmittel für den täglichen Informationsaustausch zur Verfügung.
- Er errichtete in der lokalen Vertretung eine geschützte und sichere Arbeitsumgebung, die der sensitiven Arbeit angemessen war.
- Er stellte dem Schweizer Botschafter permanent einen Mitarbeiter zur Verfügung, um die Verbindung mit dem lokalen Nachrichtendienst sowie den Vertretern anderer Nachrichtendienste zu gewährleisten und um die Informationslage dauernd zu analysieren.
- Er unterstützte das Krisenmanagement-Zentrum mit einer internen Zelle für die Lagebeurteilung, die Kontaktaufnahme mit anderen ausländischen Nachrichtendiensten und die Zusammenarbeit mit anderen Schweizer Dienststellen.
- Er stellte die Verhandlungs- und Kommunikationsbasis mit dem zuständigen ausländischen Nachrichtendienst sicher.

Private werden hingegen nur ausnahmsweise und in Fällen unterstützt, in welchen auch ein nachrichtendienstliches und damit auch ein öffentliches Interesse an der Unterstützung besteht. So kann es in einem Entführungsfall notwendig sein, auch einen Angehörigen der entführten Person mit chiffrierten Kommunikationsmitteln auszustatten. In besonderen Fällen kann auch ein nachrichtendienstliches Interesse

daran bestehen, bei einem privaten Unternehmen mit dessen Zustimmung Räume nach illegalen Abhörvorrichtungen («Wanzen») zu untersuchen. Massgeblich ist hier aber das staatliche Interesse an der Leistung, nicht der Wunsch des Privaten. Der NDB soll insbesondere nicht in Konkurrenz mit privaten Anbietern von vergleichbaren Dienstleistungen treten. Geht es um die Wahrung wesentlicher Landesinteressen nach Artikel 3, kann auch der Bundesrat den NDB mit solchen Dienstleistungen beauftragen.

Es erscheint richtig, für diese Unterstützungen und ihre Einschränkungen eine ausdrückliche gesetzliche Grundlage zu schaffen.

Art. 69 Politische Steuerung durch den Bundesrat

Der NDB ist ein Instrument, das in besonderem Mass den Landesinteressen und der Landesregierung dient. Die Rolle des Bundesrates in der politischen Steuerung und Ausrichtung der Tätigkeiten des NDB soll deshalb im NDG nicht nur aus den bisherigen Rechtsgrundlagen übernommen, sondern verdeutlicht und zusätzlich gestärkt werden. Artikel 69 nimmt deshalb verschiedene Elemente der bisherigen Gesetzgebung auf und fasst sie in einer zentralen Bestimmung über die politische Steuerung zusammen. Die Geschäftsprüfungsdelegation hat selbstverständlich wie zu allen anderen Unterlagen, vollen Zugang zu den erwähnten politischen Steuerungsinstrumenten.

Buchstabe a führt das heute schon bestehende System weiter, wonach der Bundesrat dem NDB einen strategischen Grundauftrag erteilt. Dieser hält sich an den Rahmen des Gesetzes, gibt aber thematische und regionale Prioritäten vor. Der NDB ist wegen seiner geringen Grösse vor allem im Auslandsbereich nicht in der Lage, sämtliche Regionen und sicherheitspolitischen Entwicklungen gleichermassen abzudecken. Der strategische Grundauftrag des Bundesrates gibt ihm hier deshalb die Richtung vor. Zusätzlich können natürlich kurzfristige Ereignisse und Entwicklungen die Tätigkeit des NDB innerhalb des gesetzlichen Rahmens beeinflussen. Wenn solche Entwicklungen längerfristige Auswirkungen haben, ist gegebenenfalls der Grundauftrag schon ausserhalb des ordentlichen Überprüfungszeitraums von vier Jahren anzupassen. Bei der politischen Steuerung ist jedoch grundsätzlich Kontinuität anzustreben. Eine richterliche Genehmigung, wie in der Vernehmlassung vereinzelt vorgeschlagen, ist für dieses politische Steuerungsinstrument nicht sinnvoll. Sie würde zudem die Verantwortung vom Bundesrat zum Gericht verlagern.

Gegenwärtig ist der Grundauftrag auf Stufe Verordnung geregelt (Art. 2 Abs. 2 V-NDB). Er ist aufgrund seiner Bedeutung und seines Inhalts als «geheim» klassifiziert.

Buchstabe b verweist auf die Beobachtungsliste, die in Artikel 71 ausführlich geregelt ist, und bereits aus dem geltenden Recht bekannt ist (Art. 11 Abs. 3–7 BWIS).

Buchstabe c schliesst an das neue Datenbearbeitungskonzept mit der Unterscheidung und strikteren Behandlung von Daten zum gewalttätigen Extremismus an. Damit der NDB diese Unterscheidung eindeutig handhabt, bezeichnet der Bundesrat jährlich die darunter fallenden Gruppierungen. Gegen solche Gruppierungen dürfen z.B. keine genehmigungspflichtigen Massnahmen nach den Artikeln 25 ff. durchgeführt werden. Weiter werden die Daten betreffend die gewalttätig-extremistischen Gruppierungen im Rahmen der Datenbearbeitung des NDB im speziellen Informations-

system IASA-GEX NDB abgelegt (Art. 49). Ausserdem nimmt der Bundesrat Kenntnis von der Anzahl von Personen des gewalttätig-extremistischen Spektrums, die nicht oder noch nicht einer bestimmten Gruppierung zugeordnet werden konnten. So erhält der Bundesrat ein gesamthaftes Bild des Gewaltextremismus in der Schweiz.

Wie schon nach geltendem Recht genehmigt der Bundesrat nach *Buchstabe f* die Zusammenarbeit des NDB mit Sicherheitsorganen anderer Staaten. Gemeint sind hier in erster Linie jene Nachrichtendienste, mit denen der NDB institutionalisierte Kontakte unterhält. Diese Kontakte werden auf einer speziellen Liste zusammengefasst, die das VBS dem Bundesrat zur Genehmigung beantragt.

Die vom Bundesrat zu genehmigende Zusammenarbeit mit ausländischen Behörden ist im Bereich des Nachrichtendienstes klassischerweise nicht formell geregelt, z.B. durch Staatsverträge. Es handelt sich meistens um nicht verpflichtende, formlose Agreements oder Absprachen auf Verwaltungsebene.

Der Anschluss des NDB an eine gemeinsame Datenbank, die im Verbund mit ausländischen Nachrichtendiensten des NDB betrieben würde, müsste hingegen gemäss *Absatz 3* in einem vom Bundesrat abzuschliessenden völkerrechtlichen Abkommen geregelt werden. Derzeit bestehen weder solche Datenbanken, noch entsprechende Abkommen, jedoch gibt es immer wieder Überlegungen auf internationaler Ebene, die Zusammenarbeit durch solche Instrumente zu verbessern. Im Zusammenhang mit den aktuellen Fragen um die internationalen Abhörpraktiken grosser ausländischer Nachrichtendienste wird unter anderem auch diskutiert, die gegenseitigen nachrichtendienstlichen Tätigkeiten künftig staatsvertraglich zu regeln (z.B. «No-spy-Abkommen»). Es ist derzeit noch zu früh, um zu beurteilen, ob sich hier international tatsächlich eine neue Praxis entwickeln wird, die auch zu verpflichtenden und durchsetzbaren Regeln führt. Der Bundesrat hält es für angebracht, bei einer Neukodifizierung des Nachrichtendienstes Vorbereitungen zu treffen, damit sich die Schweiz künftig allenfalls an solchen Entwicklungen beteiligen kann. Der Bundesrat geht davon aus, dass bis auf weiteres eher nur untergeordnete technische Fragen Bestandteil von Abkommen im Bereich des Nachrichtendienstes sein werden.

Art. 70 Wahrung wesentlicher Landesinteressen

Dieser Artikel knüpft an Artikel 3 an und legt das Verfahren fest, mit welchem der NDB in besonderen Lagen mit Massnahmen zur Wahrung wesentlicher Landesinteressen beauftragt werden kann. Der NDB erhält auf diesem Weg weder zusätzliche Befugnisse, noch werden die Bestimmungen über die Genehmigungspflicht für bestimmte Beschaffungsmassnahmen aufgehoben. Die formelle Beauftragung ist vielmehr eine Voraussetzung dafür, dass der NDB überhaupt in einem Bereich tätig werden darf, der über den normalen Aufgabenbereich gemäss Gesetz und Grundauftrag hinausgeht.

Art. 71 Beobachtungsliste

Die schon aus dem BWIS bekannte Beobachtungsliste ist ein Führungsinstrument des Bundesrates. Die Liste wird vom VBS erstellt und ist vom Bundesrat jährlich zu genehmigen (Art. 69 Abs. 1 Bst. b). Seit dem 11. September 2001 geht die internationale Gemeinschaft verstärkt gegen den Terrorismus vor. Durch den Einbezug der internationalen Listen im Rahmen von «BWIS II reduziert» wurde der Bezug auf

internationale Terrorlisten als Massstab für die Beobachtungsliste festgelegt. Im Unterscheid zum BWIS, das den Bundesrat beauftragt, die relevanten internationalen Organisationen und Gemeinschaften zu bezeichnen, nennt das NDG in *Absatz 2* nur noch die Vereinten Nationen (UNO) und die EU. Es ist kaum zu erwarten, dass andere internationale Organisationen Listen von vergleichbarer Bedeutung erlassen werden.

Mit der Aufnahme einer Organisation oder Gruppierung in die schweizerische Beobachtungsliste sind keine Sanktionen (z.B. Organisationsverbot) wie beim Listensystem des UN-Sicherheitsrates nach der Resolution Nr. 1267[34] verbunden. Im Gegensatz zur Liste des UN-Sicherheitsrates werden in die Beobachtungsliste auch keine Einzelpersonen aufgenommen. Die Aufnahme einer Organisation, Gruppierung (oder Person) auf eine internationale Liste führt nicht automatisch dazu, dass sie auch in die schweizerische Beobachtungsliste überführt werden muss. Wenn offensichtlich ist, dass eine bestimmte Organisation oder Gruppierung für die Schweiz ohne Relevanz ist, kann von einer Aufnahme abgesehen werden. Andere international gelistete Organisationen oder Gruppierungen können aber ohne weitere Begründung auf die schweizerische Beobachtungsliste aufgenommen werden.

Dank dem regelmässigen Genehmigungsverfahren durch den Bundesrat bleibt zudem der Handlungsspielraum gewahrt, eine Gruppierung von der Liste zu entfernen, wenn sie die innere oder äussere Sicherheit der Schweiz erwiesenermassen nicht mehr bedroht (sogenanntes Delisting).

Bei der Beobachtungsliste gilt die Bearbeitungsschranke nach Artikel 5 Absatz 5 (politische Betätigung und Ausübung von Grundrechten) nicht (vgl. Art. 5 Abs. 8). Der NDB kann über Organisationen und Gruppierungen, die in der Liste enthalten sind, alle verfügbaren Informationen beschaffen und bearbeiten, wenn diese dazu beitragen können, die Bedrohung zu beurteilen, die von diesen Vereinigungen ausgeht. Weitere unmittelbare Auswirkungen im Sinne von Sanktionen, Verboten oder ähnlichem bestehen für die betroffenen Organisationen oder Gruppierungen aber nicht. Solche sind gegebenenfalls weiterhin in besonderen Verfügungen oder Verordnungen zu erlassen, die nicht in der Kompetenz des Nachrichtendienstes liegen.

Art. 72 Tätigkeitsverbot

Diese Bestimmung entspricht inhaltlich praktisch unverändert Artikel 9 BWIS in der Fassung gemäss Änderung vom 23. Dezember 2011 («BWIS II reduziert»).

Die Bestimmung regelt die gesetzliche Kompetenz des Bundesrates in den vom NDG vorgesehenen Fällen, schränkt aber dessen allgemeine Kompetenz zum Erlass von Verordnungen und Verfügungen gestützt auf Artikel 185 Absatz 3 BV bei schweren anderen Störungen der öffentlichen Ordnung oder der inneren oder äusseren Sicherheit nicht ein. Diese Befugnis des Bundesrates bleibt in den Fällen, die durch das Gesetz nicht geregelt sind, parallel weiter bestehen.

Die vorgeschlagene Bestimmung schafft die Möglichkeit, dass der Bundesrat im Bereich der inneren oder äusseren Sicherheit ein Tätigkeitsverbot für maximal fünf Jahre erlassen und dieses jeweils um weitere fünf Jahre verlängern kann, sofern die

34 Die Resolution 1267 (1999) betreffend Afghanistan kann im Internet in französischer Sprache unter folgender Adresse abgerufen werden:
www.un.org/fr > Conseil de sécurité > Douments > Résolutions > 1999

Voraussetzungen dafür weiterhin erfüllt sind. Mit Hilfe dieser neuen Bestimmung könnte der Bundesrat beispielsweise Tätigkeitsverbote für Ableger von Terrororganisationen verfügen. Für die Al-Qaïda besteht gegenwärtig eine Ende 2014 auslaufende Verordnung der Bundesversammlung, die die Al-Qaïda als Organisation verbietet. Es wird zu beurteilen sein, ob hier künftig besser Tätigkeitsverbote nach Artikel 9 BWIS bzw. dem NDG zu erlassen sind oder ob das Parlament Organisationsverbote aufgrund seiner Verordnungskompetenz erlässt bzw. verlängert.

Gestützt auf die Erfahrungen, die in der Vergangenheit gemacht wurden, ist von sehr wenigen Fällen pro Jahr auszugehen. Der mit solchen Verboten verbundene Aufwand kann deshalb nicht separat ausgewiesen werden, sondern bewegt sich im Rahmen der üblichen politischen Geschäfte.

Es handelt sich dabei um eine präventive Massnahme, die schwerere Bedrohungen der Sicherheit oder auch Straftaten verhindern soll. Liegt bereits der Verdacht auf strafbare Handlungen vor, ist ein ordentliches Strafverfahren durchzuführen; allfällige präventive Verbote müssten mit der zuständigen Strafverfolgungsbehörde eng abgesprochen werden, um ein laufendes Strafverfahren nicht zu gefährden. Es kann aber auch in solchen Fällen sinnvoll sein, flankierend präventive Massnahmen anzuordnen, um die innere oder äussere Sicherheit zu gewährleisten.

Der Bundesrat erhält nach *Absatz 1* die Kompetenz, gegen Tätigkeiten, mit denen eine konkrete Bedrohung der inneren oder äusseren Sicherheit der Schweiz einhergeht, ein verwaltungsrechtliches Verbot zu verhängen. Alle Departemente sollen entsprechende Anträge stellen können.

Umfang und Inhalt der verbotenen Tätigkeiten sind im Beschluss so genau wie möglich zu umschreiben, damit das Verbot wirkungsvoll umgesetzt und kontrolliert werden kann. Sie hängen jedoch von den Aktivitäten der Betroffenen im Einzelfall ab und sind deshalb im Gesetz nicht abschliessend zu beschreiben.

Verbote nach *Absatz 1* können die Betroffenen an der Ausübung von Grundrechten hindern, weshalb sie nach *Absatz 2* zu befristen sind. Die Behörden werden dadurch verpflichtet, nach Ablauf der Gültigkeit eines Verbotes wiederum zu prüfen, ob die Anordnungsvoraussetzungen nach wie vor erfüllt oder hinfällig geworden sind.

Sind die Anordnungsvoraussetzungen noch erfüllt, kann die Gültigkeitsdauer eines Verbots jeweils um weitere fünf Jahre verlängert werden, und zwar so lange, als es die Umstände erfordern. Ist keine Verlängerung notwendig, verfällt das Verbot automatisch.

Gestützt auf diesen Artikel verfügte Tätigkeitsverbote können nach Artikel 79 beim Bundesverwaltungsgericht im Verfahren gemäss dem Verwaltungsverfahrensgesetz vom 20. Dezember 1968[35] angefochten und anschliessend an das Bundesgericht weitergezogen werden.

6. Kapitel, 2. Abschnitt

Die Artikel 73–77 enthalten in aufsteigender Reihenfolge die Kaskade der Aufsichts- und Kontrollvorschriften:

1. Selbstkontrolle durch den NDB
2. Aufsicht und Kontrolle durch das VBS

35 SR **172.021**

3. Unabhängige Kontrollinstanz
4. Aufsicht und Kontrolle durch den Bundesrat
5. Parlamentarische Kontrolle

Die einzelnen Kontrollstufen und -elemente entsprechen im Wesentlichen dem geltenden Recht (Art. 4*b* ZNDG, Art. 25 ff. BWIS und Art. 31 ff. V-NDB).

Die UKI stellt die Rechtmässigkeit der Funkaufklärung über das Ausland nach Artikel 37 sicher.

Neu wird auch für die kantonale parlamentarische Aufsicht eine Regelung vorgeschlagen, die klar abgegrenzte Zuständigkeiten für die Aufsicht des Bundes und der Kantone schafft (Art. 78 Abs. 2). Damit werden sowohl Doppelzuständigkeiten als auch Lücken in der Aufsicht vermieden.

Nicht speziell aufgenommen hat der Bundesrat das in der Vernehmlassung vereinzelt gestellte Begehren, dass auch die Wirtschaftlichkeit der nachrichtendienstlichen Tätigkeiten zu überprüfen sei. Dies ist bereits durch die allgemeinen Bestimmungen über die finanzielle Aufsicht der Bundesbehörden sichergestellt und wird durch die neue Erwähnung der Finanzdelegation in Artikel 77 noch verstärkt. Zudem darf sich die Gewährleistung der inneren oder äusseren Sicherheit nur beschränkt an Aspekten der Wirtschaftlichkeit orientieren. Gemessen an den Zweckbestimmungen dieses Gesetzes – beispielsweise der Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz, der Sicherheit ihrer Bevölkerung und der Schweizerinnen und Schweizer im Ausland oder der Wahrung der Handlungsfähigkeit der staatlichen Organe – tritt eine monetäre Beurteilung oft in den Hintergrund.

Art. 74 Aufsicht durch das Departement

Wie bis anhin soll das VBS eine interne Aufsichtsinstanz, die nachrichtendienstliche Aufsicht, zur Ausübung der Fachaufsicht über die Nachrichtendienste unterhalten. Diese wird neu auf Gesetzesstufe geregelt (Abs. 2), weil ihr erweiterte Befugnisse zugeteilt werden sollen.

Ein eigenes Kontrollorgan innerhalb des Departements erscheint im Gefüge der Aufsichtsorgane zwingend, da der Bundesrat andernfalls im Verhältnis zur parlamentarischen Oberaufsicht seine Aufsicht nicht vollumfänglich eigenständig wahrnehmen könnte. Der internen Aufsichtsinstanz stehen umfassende Einsichts- und Auskunftsrechte zu.

In Bezug auf die Eingliederung der Aufsichtsinstanz sind mehrere Möglichkeiten denkbar: eine Zuordnung zur Geschäftsprüfungsdelegation beider Räte (ähnlich der parlamentarischen Verwaltungskontrolle gegenüber den Geschäftsprüfungskommissionen), administrativ zur Bundeskanzlei als Stabsorgan des Bundesrates oder weiterhin (ebenso rein administrativ) zum Generalsekretariat VBS; gemäss der letztgenannten Variante berichtete die Aufsichtsinstanz der Chefin oder dem Chef des VBS unter Abgabe von Empfehlungen direkt. Der Bundesrat ist der Auffassung, dass die Zuordnung mit einer direkten und unbeeinflussten Rapportierung an den Departementschef oder die Departementschefin, der oder die persönlich und unmittelbar die oberste departementale Verantwortung trägt, der staatspolitischen Führungsverantwortung und -zurechenbarkeit am besten gerecht wird.

Innerhalb der Bundesverwaltung existiert kein mit dem Nachrichtendienst vergleichbares Bundesamt, das überwiegend ohne Wissen der Betroffenen in deren

Grundrechte, insbesondere in die Privatsphäre und die informationelle Selbstbestimmung, einzugreifen befugt ist. Mit der Schaffung der internen Aufsichtsinstanz nahm der Bundesrat parallel zur Schaffung des Nachrichtendienstes des Bundes per 1. Januar 2010 ein Anliegen des Parlaments auf, das eine umfassende, ständige Kontrolle der Nachrichtendienste wünschte. Die interne Aufsichtsinstanz ist insofern im Bundesverwaltungsrecht ein Unikat.

Mindestens jährlich erstellt die interne Aufsichtsinstanz einen vertraulichen Kontrollplan, der mit der Geschäftsprüfungsdelegation beider Räte abzustimmen und der Chefin oder dem Chef des VBS zur Genehmigung vorzulegen ist. Die Chefin oder der Chef des VBS kann der internen Kontrollinstanz zusätzliche, anlassbezogene Kontrollaufträge erteilen. Zwecks Verstärkung der Unabhängigkeit und Wirksamkeit der Aufsicht und in Umsetzung einer Empfehlung der Geschäftsprüfungsdelegation beider Räte soll die notwendige Regelung neu auf die formellgesetzliche Stufe gehoben werden. In der entsprechenden Norm über die interne Aufsichtsinstanz werden demzufolge ihr Status, ihre Kompetenzen und ihre Weisungsungebundenheit festgelegt. Die Bestimmungen des RVOG bleiben anwendbar.

Auch die Kontrolltätigkeit der internen Aufsichtsinstanz bei den kantonalen Vollzugsbehörden soll gesetzlich geregelt werden (Abs. 3). Dies gilt für jene Bereiche, in denen die Kantone gestützt auf Bundesaufträge Informationen beschaffen (vgl. Art. 81). Auf diese Weise wird die Kontroll- und Steuerungsaufgabe des VBS nach Absatz 1 ergänzt.

Vereinzelt war in der Vernehmlassung vorgeschlagen worden, die departementale Aufsichtsinstanz durch ein aussenstehendes, völlig unabhängiges Gremium zu ersetzen. Der Bundesrat hält eine solche, völlig neuartige Aufsicht für nicht sachgerecht. Sie würde die gesetzliche Aufsichtspflicht und Verantwortung der Chefin oder des Chefs des VBS tangieren und würde auch weitere Fragestellungen nach der politischen Führung durch Bundesrat und Departement nach sich ziehen. Das vorgeschlagene Aufsichtssystem entspricht hingegen den bestehenden Grundlagen des RVOG aber auch des Verantwortlichkeitsgesetzes und ist geeignet, eine wirksame Aufsicht zu gewährleisten.

Art. 75 Unabhängige Kontrollinstanz für die Funkaufklärung

Die Regelung über die unabhängige Kontrollinstanz (UKI) entspricht wie jene über die Funkaufklärung (Art. 37) weitgehend der am 1. November 2012 in Kraft getretenen Regelung, welche das Parlament direkt im ZNDG verankert hat (Art. 4*b* ZNDG; vgl. auch Ausführungen zu Art. 37). Es handelt sich heute um eine verwaltungsintern besetzte Kommission. Das ZNDG schliesst aber eine verwaltungsexterne Besetzung nicht aus, was beispielsweise für eine bestimmte Zeit sinnvoll sein kann, wenn ein fachkundiges Mitglied der UKI die Bundesverwaltung verlässt.

Die Kontrolltätigkeit der UKI war schon zuvor analog in der Verordnung über die elektronische Kriegführung geregelt und hat sich in den vergangenen Jahren bewährt. Sie entspricht einem Bedürfnis in einem sensiblen Bereich der Auslandsaufklärung. Die Aufgaben der UKI bei der Überprüfung der Aufträge und ihrer Bearbeitung sind in Absatz 2 geregelt. Die Bearbeitung kann und soll sie dabei wie bisher nicht umfassend kontrollieren, sondern mit geeigneten Überprüfungen sicherstellen, dass sowohl der durchführende Dienst als auch der die Ergebnisse empfangende NDB die gesetzlichen Vorschriften einhalten.

Für die Kabelaufklärung gelten vergleichbare Bestimmungen, hingegen ist dort eine dem Verfahren für genehmigungspflichtige Beschaffungsmassnahmen angeglichene richterliche und politische Genehmigung vorgesehen, weil der Vollzug der Beschaffung die Mitwirkung privater Anbieterinnen von Fernmeldediensten in der Schweiz erfordert. Dies ist bei der Funkaufklärung, die von den Bundesbehörden (ZEO und NDB) selbstständig vollzogen werden kann, nicht der Fall.

Eine zusätzliche Kontrolle der Kabelaufklärung durch die UKI würde hingegen die Verantwortungsbereiche der Beteiligten (Bundesverwaltungsgericht und Chefin oder Chef des VBS einerseits und UKI andererseits) verwischen und ist deshalb nicht sachgerecht.

Art. 76 Aufsicht und Kontrolle durch den Bundesrat

Dieser Artikel übernimmt die bereits in Artikel 26 BWIS verankerte und durch Artikel 8 ZNDG für den gesamten Nachrichtendienst anwendbar erklärte Überprüfung der Tätigkeiten auf Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit. Das NDG führt hier den bestehenden Standard an Aufsicht und Kontrolle weiter. Hierzu gehört auch die regelmässige Information des Bundesrates über die Erkenntnisse der Aufsichtsorgane des VBS und der Geschäftsprüfungsdelegation.

Art. 77 Parlamentarische Oberaufsicht

Die bisherige Regelung nach Artikel 25 BWIS wird dem Grundsatz nach übernommen und gleichzeitig präzisiert: Die parlamentarische Oberaufsicht über den Vollzug des vorliegenden Gesetzes obliegt ausschliesslich der Geschäftsprüfungsdelegation und der Finanzdelegation der eidgenössischen Räte in ihren jeweiligen Zuständigkeitsbereichen. Diese Kontrolle umfasst sowohl die Tätigkeiten des NDB als auch diejenigen der kantonalen Vollzugsbehörden, soweit letztere im direkten Auftrag des Bundes tätig sind, das heisst aufgrund eines konkreten Auftrages des NDB. Tätigkeiten der Kantone aufgrund der Beobachtungsliste (Art. 71) gehören ebenfalls zu den direkten Aufträgen, da die Beobachtungsliste jeweils jährlich den Kantonen zugestellt wird mit der Aufforderung, jegliche Informationen über die aufgeführten Organisationen und Gruppierungen zu beschaffen und an den NDB weiterzuleiten.

Tätigkeiten der kantonalen Vollzugsbehörden, die diese hingegen selbstständig in direkter Anwendung des NDG vornehmen, können neu der Oberaufsicht durch die kantonalen Parlamente unterstehen. So werden sowohl Doppelzuständigkeiten als auch Lücken in der Aufsicht vermieden. Das Informationssystem INDEX NDB (Art. 50) wird spezielle Gefässe für die Kantone enthalten, in welchen sie ihre Informationen ablegen können und welche die klare Unterscheidung der beiden Aufsichtsbereiche ermöglichen werden.

Für die Tätigkeiten der kantonalen Vollzugsbehörden im direkten Auftrag des Bundes ist der Bundesrat der Auffassung, dass der Bundesgesetzgeber mit der Schaffung der Geschäftsprüfungs- und der Finanzdelegation für die Überwachung der Tätigkeit im nachrichtendienstlichen Bereich und der Zuweisung von besonderen Kompetenzen an diese Delegationen in den Artikeln 51 und 53 des Parlamentsgesetzes vom 13. Dezember 2002[36] eine abschliessender Regelung der parlamentarischen Ober-

36 SR **171.10**

aufsicht getroffen hat. Es wäre nicht konsequent, wenn der Bundesgesetzgeber den Kantonen parallele Kompetenzen auf kantonaler Ebene einräumen würde.

Art. 78 Kantonale Aufsicht

Vorgeschlagen wird eine Teilung der Aufsicht über die kantonalen Vollzugsbehörden durch Bund und Kantone.

Aufsicht durch den Bund

Die Oberaufsicht über den Vollzug der Bundesaufträge nach diesem Gesetz und somit auch über die entsprechenden Tätigkeiten der kantonalen Vollzugsbehörden obliegt der Geschäftsprüfungsdelegation der eidgenössischen Räte. Die interne Aufsichtsinstanz des VBS kann zudem Kontrollen bei den kantonalen Vollzugsbehörden durchführen (Art. 74 Abs. 3).

Aufsicht durch die Kantone

Die Aufsicht der Kantone besteht einerseits in der Dienstaufsicht durch die Vorgesetzten der kantonalen Vollzugsbehörden. Die kantonale Dienstaufsicht überprüft:

- ob die kantonalen Verwaltungsabläufe den massgebenden Rechtsvorschriften entsprechen;
- ob die kantonale Vollzugsbehörde die Bundesdaten getrennt von den kantonalen Daten bearbeitet;
- wie die Vollzugsbehörde die vom Bund erteilten Aufträge erledigt;
- wo und wie die Vollzugsbehörde die Informationen beschafft;
- ob die Vollzugsbehörde die datenschutzrechtlichen Anforderungen (Datensicherheit, Persönlichkeitsschutz) einhält.

Diese Aufgabenteilung entspricht dem geltenden Recht (Art. 6 Abs. 3 BWIS und Art. 35 V-NDB) und hat sich in der Praxis bewährt. Sie soll deshalb beibehalten werden.

Die Bestimmungen über die kantonale Aufsicht sehen andererseits auch die Unterstützung der kantonalen Dienstaufsicht durch Aufsichtsorgane des Bundes (z.B. durch ein Aufsichtsorgan analog der heutigen nachrichtendienstlichen Aufsicht) und den Zugang zu sachdienlichen Informationen durch die kantonale Dienstaufsicht (Abs. 3) vor.

Im Rahmen der Evaluation einer geeigneten Lösung für die Aufsicht über die kantonalen Vollzugsbehörden wurden folgende Alternativen geprüft:

a. Eine *integrale Bundeslösung:* Diese würde bedeuten, dass die gesamte Aufsicht über die kantonalen Vollzugsbehörden dem Bund bzw. dem NDB übertragen würde. Diese Einheitslösung würde sämtliche Aspekte der Aufsicht umfassen, insbesondere die Dienst- und Datenschutzaufsicht. Der Bund wäre nach diesem Modell allein zuständig, entsprechende Rechtsvorschriften zu erlassen. Die bisher dem Kanton unterstellten Bediensteten, die sich mit dem Vollzug des BWIS befassen, würden in die Bundesverwaltung übernommen.

b. Eine *integrale kantonale Lösung:* Gegenüber der heutigen Lösung würde dies bedeuten, dass dem Bund keinerlei Zuständigkeit für die Aufsicht über

die kantonalen Vollzugsbehörden mehr zukommen würde, auch die Oberaufsicht der Geschäftsprüfungsdelegation der eidgenössischen Räte über die kantonalen Vollzugsbehörden würde entfallen. Im Bereich der Datenschutzaufsicht müsste die kantonale Aufsicht über umfassende Einsichtsbefugnisse in jene Daten verfügen, die von der kantonalen Vollzugsbehörde bearbeitet werden.

Die *Bundeslösung* hätte den Vorteil, dass die Aufsicht über die kantonalen Vollzugsbehörden einheitlich geregelt wird. Sie stünde aber im Widerspruch zum föderalen Konzept der inneren Sicherheit, wonach Bund und Kantone gemeinsam je in ihrem Zuständigkeitsgebiet für die Sicherheit des Landes und den Schutz der Bevölkerung zuständig sind (Art. 57 Abs. 1 BV). Die Einführung einer reinen Bundeslösung würde dem föderalistischen Aufbau unseres Staatswesens widersprechen und hätte nicht die tiefe lokale Verankerung bei den Sicherheitsbehörden. Sie ist deshalb abzulehnen.

Eine *rein kantonale Lösung* der Aufsicht über die kantonalen Vollzugsbehörden hätte ebenfalls den Vorteil, dass die Aufsicht für alle Kantone einheitlich geregelt würde. Die Zweiteilung Bund/Kantone in der Aufsicht würde entfallen. Die Zuständigkeit für die Aufsicht läge allein beim Kanton. Diese Lösung hätte allerdings den Nachteil, dass die kantonalen Parlamente, denen neu die umfassende Oberaufsicht über die Tätigkeit der kantonalen Vollzugsbehörden zufallen würde, unterschiedliche Praktiken entwickeln könnten. Zudem müssten im Fall einer rein kantonalen Lösung die kantonalen Aufsichtsorgane umfassenden Zugriff auf die Daten des Bundes haben, die von den kantonalen Vollzugsbehörden bearbeitet werden. Anders könnten sie ihre integrale Aufsichtsfunktion nicht wahrnehmen. Damit würden sie aber zwangsläufig in die Aufsichtssphäre der Bundesaufsicht eindringen und gegebenenfalls in Konflikt mit den Bundesaufsichtsorganen geraten. Es würden sich schwierige Abgrenzungsfragen bezüglich der Aufsicht über die Auftragserteilung des Bundesorgans ergeben. Der NDB würde in Teilen auch den kantonalen Aufsichtsorganen gegenüber rechenschaftspflichtig, was wiederum systemwidrig wäre. Auch die kantonale Lösung vermag deshalb insgesamt nicht zu überzeugen.

Aus diesen Gründen soll an der bisherigen geteilten Aufsicht von Bund und Kantonen festgehalten werden.

Das Prinzip der geteilten Aufsicht ist im Übrigen nichts Ungewöhnliches. Es findet sich nicht nur im Bereich des Nachrichtendienstes: In den meisten Kantonen untersteht die Kriminalpolizei nämlich organisatorisch und dienstrechtlich dem Polizeikommando. Führt sie jedoch im Auftrag der Justizbehörden Ermittlungshandlungen durch, so steht sie unter der fachlichen Aufsicht der Justizbehörden.

Mit *Absatz 2* wird neu aber der Aufsichtsbereich definiert und abgegrenzt, der von den kantonalen parlamentarischen Organen beaufsichtigt werden kann. Es handelt sich um diejenigen Tätigkeiten der kantonalen Vollzugsbehörden, die diese im direkten Vollzug des NDG auf ihrem Gebiet vornehmen, ohne dass sie im Einzelfall hierzu einen ausdrücklichen Auftrag des NDB erhalten haben. Artikel 81 Absatz 1 enthält hierzu den Verweis auf die entsprechenden Kompetenzen der Kantone, selbstständig Beschaffungsmassnahmen zu ergreifen. Diese Neuordnung ist sinnvoll, da die Bundesorgane von solchen Tätigkeiten der Kantone in der Regel keine Kenntnis haben und es deshalb schwieriger ist, sie in Aufsichtstätigkeiten zu erfassen. Mit einer Zuweisung an die kantonale Ebene werden so allfällige Lücken vermieden, es entstehen aber auch keine Doppelspurigkeiten. Für das Bearbeiten der

entsprechenden Daten und ihre Kontrolle wird das Informationssystem INDEX NDB entsprechende Gefässe enthalten.

Die kantonalen Parlamente bleiben selbstverständlich in jenen Bereichen autonom, in denen die kantonalen Vollzugsbehörden ausserhalb des NDG für die innere Sicherheit ihres Gebietes tätig sind. Das NDG verlangt hier nicht, dass diese ausschliesslich für seinen Vollzug eingesetzt werden. In der Regel gibt es nützliche Synergien beim Vollzug des NDG und der kantonalen Polizeigesetzgebung, die der Bund nicht unterbinden will.

Art. 79 Rechtsschutz

Das NDG ermöglicht teilweise einschneidende Massnahmen und Verfügungen, für die ein angemessener Rechtsschutz sichergestellt sein muss. Das NDG sieht hier in *Absatz 1* den ordentlichen Rechtsweg an das Bundesverwaltungsgericht und danach an das Bundesgericht vor. Die Massnahmen fallen damit klarerweise nicht unter die Ausnahmeregelung von Artikel 83 Buchstabe a des Bundesgerichtsgesetzes vom 17. Juni 2005[37], der Entscheide auf dem Gebiet der inneren oder äusseren Sicherheit des Landes von der Beschwerde in öffentlich-rechtlichen Angelegenheiten ausnimmt.

Absatz 2 bestimmt, dass Beschwerden gegen Verfügungen des NDB über die besondere Auskunftspflicht Privater (Art. 24) keine aufschiebende Wirkung haben. Nach Artikel 55 Absatz 1 des Verwaltungsverfahrensgesetzes haben Beschwerden aufschiebende Wirkung, sofern diese nicht ausdrücklich entzogen wird. Müsste für das Erlangen benötigter Auskünfte jedoch jeweils der Ausgang eines Beschwerdeverfahrens abgewartet werden, könnten Bedrohungen für die innere oder äussere Sicherheit meistens nicht rechtzeitig beurteilt werden. Das NDG sieht deshalb hier als *lex specialis* keine aufschiebende Wirkung vor.

Absatz 3 verhindert, dass für die Sicherheit des Landes notwendige Auskünfte an den NDB durch Beschwerden so lange verzögert werden können, dass die Bedrohung nicht mehr abgewendet werden kann.

Da die Mitteilung einer genehmigungspflichtigen Beschaffungsmassnahme unter Umständen erst lange nach ihrer Beendigung erfolgt (z.B. um weitere laufende Beschaffungsmassnahmen nicht zu gefährden), legt *Absatz 3* den Beginn der Beschwerdefrist auf den Erhalt der Mitteilung fest.

Das Bundesverwaltungsgericht hatte in der Vernehmlassung Bedenken geäussert, die Funktionen als Genehmigungsinstanz für gewisse Massnahmen und später als Beschwerdeinstanz im Beschwerdeverfahren im selben Gericht anzusiedeln. Es schlug vor, stattdessen das Bundesstrafgericht als Beschwerdeinstanz vorzusehen. Der Bundesrat will jedoch die klare Trennung zwischen verwaltungsrechtlichen und strafprozessrechtlichen Instanzen beibehalten und die rechtliche und sachliche Kompetenz für die Beurteilung nachrichtendienstlicher Sachverhalte im Bundesverwaltungsgericht konzentrieren. Allfällige Interessenkonflikte zwischen genehmigenden Abteilungsvorsitzenden als Genehmigungsinstanz und Abteilungen als Beschwerdeinstanz können durch eine geeignete Zuständigkeitsorganisation innerhalb des Bundesverwaltungsgerichts vermieden werden. Die Vorteile der Konzentration des Verfahrens auf den verwaltungsrechtlichen Bereich überwiegen klar.

37 SR **173.110**

Art. 80 Ausführungsbestimmungen

Gemäss Artikel 7 RVOG erlässt der Bundesrat die Verordnungen, soweit er dazu durch Verfassung oder Gesetz ermächtigt ist (vgl. auch Art. 182 Abs. 1 BV). Artikel 80 beauftragt den Bundesrat zusätzlich zu den besonderen Delegationen im Gesetz, allgemeine Vollzugsvorschriften zu erlassen.

Art. 81 Vollzug durch die Kantone

Zunächst wird in Absatz 1 der Grundsatz statuiert, dass die Kantone auf ihrem Gebiet gemeinsam mit dem Bund für den Vollzug des vorliegenden Gesetzes sorgen. In grundsätzlicher Hinsicht ist zur Aufgabenteilung Bund/Kantone im Bereich der inneren Sicherheit Folgendes zu bemerken:

Artikel 57 BV enthält zwar die inhärente Kompetenz des Bundes, dort für seine innere Sicherheit zu sorgen und gesetzliche Bestimmungen zu erlassen, wo es um die Wahrnehmung von eigentlichen Bundeszuständigkeiten geht (Massnahmen zu seinem eigenen Schutz bzw. zum Schutz seiner Institutionen und Organe). Der Bund hat jedoch nur eine sektorielle und keine umfassende Rechtsetzungskompetenz im Bereich der inneren Sicherheit (vgl. Bericht des Bundesrates vom 2. März 2012[38] in Erfüllung des Postulats Malama vom 3. März 2010 «Innere Sicherheit. Klärung der Kompetenzen»). Die Kantone sind demnach frei, im Bereich des Nachrichtendienstes eigene Tätigkeiten zu entfalten und gesetzliche Bestimmungen zu erlassen, soweit es sich nicht um Bereiche handelt, in denen die Regelungskompetenz beim Bund liegt (originäre oder inhärente Kompetenz). Die Regelungskompetenz des Bundes betreffend die Wahrung der inneren Sicherheit wird in der vorliegenden Vorlage konkretisiert.

Der Bericht äussert sich zum Thema der Zuständigkeit der Kantone wie folgt (vgl. S. 4479/4480):

«… Die Zuständigkeit der Kantone, auf ihrem Hoheitsgebiet für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung zu sorgen, gilt als originäre Kompetenz der Kantone. Die Kantone verfügen auf ihrem Territorium über die Polizeihoheit und damit über die entsprechende Rechtsetzungskompetenz im Hinblick auf die Wahrnehmung des umfassenden Gefahrenabwehrauftrags. Der Grundsatz der primären Verantwortung der Kantone für die Sicherheit auf ihrem Territorium ist in der Lehre wie auch in der Rechtsprechung unbestritten. Der Bundesrat seinerseits hat in konstanter Praxis festgehalten, dass die Gesetzgebung im Polizeibereich grundsätzlich den Kantonen obliege. Der Umstand, dass dem Bund kein allgemeiner Auftrag zur Gefahrenabwehr obliegt, widerspiegelt sich auch in institutioneller Hinsicht: Während jeder der 26 Kantone über ein eigenes Polizeikorps verfügt, existiert auf Bundesebene keine umfassend tätige Polizeibehörde.

Sieht die Bundesverfassung in einem bestimmten Sachbereich keine Kompetenzzuweisung an den Bund vor, so fällt die Zuständigkeit auf diesem Gebiet nach den allgemeinen Zuständigkeitsregeln den Kantonen zu. Für die Kantone bedeutet dies, dass sie alle Kompetenzen wahrnehmen dürfen, die nicht dem Bund übertragen worden sind. Wo auf dem Gebiet der Sicherheit somit keine spezifischen Kompetenzen des Bundes ausgewiesen sind, verbleibt die Kompetenz primär bei den Kantonen. Artikel 43 BV präzisiert, dass die Kantone bestimmen, welche Aufgaben und

38 BBl **2012** 4459

wie sie diese Aufgaben im Rahmen ihrer Zuständigkeiten erfüllen wollen. Dieser Grundsatz gilt indessen nicht uneingeschränkt: Die Kantone sind auch in Ausübung ihrer Zuständigkeiten nicht immer frei, ihre Aufgaben und deren Ausgestaltung zu bestimmen, namentlich dann nicht, wenn die Verfassung ihnen spezifische Aufgaben überträgt oder ihnen vorgibt, wie sie eine Aufgabe zu erfüllen haben. In diesen Fällen wird die kantonale Autonomie insoweit eingeschränkt, als die Verfassung bestimmte Anforderungen bezüglich der Erfüllung der Aufgaben stellt. Ein solches Beispiel findet sich in Artikel 57 Absatz 1 BV; auch die von der Bundesverfassung garantierten Grundrechte (Art. 35 BV) begrenzen den Handlungsspielraum der Kantone.»

Die in den *Absätzen 1 und 2* enthaltenen Grundsätze (Beschaffung von Informationen, selbstständig oder aufgrund eines Auftrags des NDB bzw. unaufgeforderte Meldung an den NDB) wurden aus dem geltenden Recht übernommen (Art. 12 BWIS). Sie haben sich in der Praxis bewährt und sollen beibehalten werden. Auf Anregung zahlreicher Kantone in der Vernehmlassung wurde Absatz 1 um einen zweiten Satz ergänzt, der eine Aufzählung enthält, welche genehmigungsfreien Beschaffungsmassnahmen des NDG die kantonalen Vollzugsbehörden zum selbstständigen Vollzug des NDG einsetzen können. Es handelt sich dabei um das Auswerten öffentlicher Quellen (Art. 13), das Beobachten an öffentlichen und allgemein zugänglichen Orten (Art. 14), das Führen von menschlichen Quellen (Art. 15), das Einholen von Auskünften oder das Entgegennehmen von Meldungen von anderen Behörden (Art. 19 und 20), das Entgegennehmen von Meldungen und das Befragen von Dritten (Art. 22 und 24). Die anderen Beschaffungsmassnahmen, insbesondere die genehmigungspflichtigen, vollziehen die kantonalen Vollzugsorgane nur im Auftrag des NDB. Sie können diesem entsprechende Anträge stellen. Weiterhin möglich sind auch Tätigkeiten der kantonalen Vollzugbehörden im Rahmen der kantonalen Polizeigesetzgebung. Deren Ergebnisse können nach Artikel 20 Absatz 1 auch in den Bereich des NDG überführt werden, wenn sie für den Vollzug des NDG erforderlich sind.

Die gegenseitige technische und operationelle Unterstützung nach den *Absätzen 3 und 4* besteht seit Jahren und ermöglicht einen effizienten Einsatz von personellen und technischen Mitteln von Bund und Kantonen.

Die Abgeltungen der Kantone nach *Absatz 5* für Leistungen beim Vollzug dieses Gesetzes entsprechen ebenfalls dem geltenden Recht (vgl. Art. 28 Abs. 1 BWIS). Der Bundesrat möchte angesichts der besonderen Vollzugssituation an dieser besonderen Abgeltung, welche die Aufwände der Kantone nur zu einem Teil deckt festhalten; Leistungen beim Vollzug des NDG sollen mit dem allgemeinen Finanzausgleich zwischen Bund und Kantonen nicht als abgegolten betrachtet werden.

Im Übrigen ergibt sich die Einhaltung der Grundsätze der Subventionsgesetzgebung einerseits aus dem Umstand, dass die Kantone von Gesetzes wegen dazu verpflichtet werden, eine Behörde zu bestimmen, die zum Vollzug mit dem NDB zusammenarbeitet bzw. grundsätzlich auf Auftrag des Bundes bzw. des NDB hin aktiv wird (Ausgestaltung bzw. materielle Steuerung; vgl. vor allem Artikel 9 des Gesetzesentwurfs und dortige Erläuterungen). Die so veranlassten Arbeiten unterstehen einer strengen Kontrolle durch Kontroll- und Aufsichtsorgane des Bundes und der Kantone (vgl. 2. Abschnitt des Gesetzesentwurfs). Andererseits erfolgt die (für die Kantone nicht kostendeckende) Abgeltung zwar pauschal, doch richtet sich der Verteilschlüssel nach der Zahl der im jeweiligen Kanton überwiegend für Bundesaufgaben tätigen Personen und erfolgt ausschliesslich im Rahmen bewilligter Kredi-

te (Transparenz und finanzielle Steuerungsmöglichkeit sind somit gewährleistet). Wie eingangs erwähnt soll damit eine bewährte und effiziente Regelung weitergeführt werden, von der abzuweichen kein Anlass besteht.

Aufhebung anderer Erlasse

Der vorliegende Entwurf übernimmt die nachrichtendienstlichen Inhalte des BWIS, nicht aber dessen polizeirechtlichen Bestimmungen (Schutz von Personen und Gebäuden, Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen, Beschlagnahmung von Gewaltpropaganda). Da die Arbeiten an einem Polizeiaufgabengesetz eingestellt wurden, muss das BWIS für die polizeirechtlichen Belange noch weiter bestehen bleiben. Zusätzlich wird es mit einzelnen neuen Bestimmungen ergänzt, die im Vorentwurf des Polizeiaufgabengesetzes in die Vernehmlassung gegeben worden waren und die für den weiteren Vollzug des restlichen BWIS notwendig sind. Das BWIS kann deshalb nicht integral aufgehoben werden, sondern nur dessen nachrichtendienstliche Teile.

Für den Bereich der Personensicherheitsprüfungen (PSP) ist mit dem künftigen Informationssicherheitsgesetz eine neue Vorlage in Vorbereitung, die diesen Bereich des BWIS übernehmen wird.

Das ZNDG wird durch das NDG hingegen vollständig erfasst und kann aufgehoben werden.

Änderung anderer Erlasse

Bundesgesetz vom 21. März 1997[39] über Massnahmen zur Wahrung der inneren Sicherheit

Vorbemerkungen

Ursprünglich war vorgesehen, die polizeilichen Bestimmungen des BWIS im neu zu schaffenden Polizeiaufgabengesetz (PolAG) zu regeln. Damit hätte das BWIS mit der Einführung des NDG ersatzlos aufgehoben werden können. Zum Vorentwurf des PolAG (VE-PolAG) ist bei den Kantonen, den politischen Parteien und weiteren Organisationen die Vernehmlassung durchgeführt worden (November 2009 bis März 2010).[40] Am 26. Juni 2013 gab der Bundesrat bekannt, die Arbeiten an diesem Gesetzesprojekt seien einzustellen; soweit nötig, solle der unbestrittene Regelungsbedarf mittels punktueller Anpassungen der bestehenden Rechtsgrundlagen umgesetzt werden. Somit bleibt das BWIS, anders als noch im Vorentwurf des NDG vorgesehen (vgl. Anhang, Änderung bisherigen Rechts, I, Ziff. 1), parallel zum neuen NDG bestehen. Sein Inhalt aber ist mit dem Inkrafttreten des NDG auf die Regelung der polizeilichen Aufgaben beschränkt, die dem Bundesamt für Polizei (fedpol) übertragen sind. Es handelt sich dabei im Besonderen um die Massnahmen gegen Gewaltpropagandamaterial sowie gegen Gewalt anlässlich von Sportveranstaltungen

39 SR **120**

40 Der Vorentwurf des Polizeiaufgabengesetzes ist im Internet abrufbar unter: www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2009 > Eidgenössisches Justiz- und Polizeidepartement

und um die sicherheitspolizeilichen Aufgaben zum Schutz von Personen und Gebäuden des Bundes sowie die Wahrnehmung der völkerrechtlichen Schutzpflichten gegenüber Personen und Gebäuden. An diesen verbleibenden Bestimmungen werden die erforderlichen redaktionellen Anpassungen vorgenommen, die sich aus der Schaffung des NDG ergeben.

Zusätzlich sollen drei neue Regelungen in das BWIS aufgenommen werden, die bereits Inhalt des VE-PolAG waren. Sie stellen Ergänzungen dar, die in direktem Zusammenhang mit den im BWIS verbleibenden sicherheitspolizeilichen Aufgaben von fedpol stehen und die deren Erfüllung gewährleisten: Es handelt sich um Artikel 13*f* (Beschlagnahme gefährlicher Gegenstände; Art. 32 VE-PolAG), 23 Absatz 3bis (Gefährderansprache, Art. 31 VE-PolAG) und 23*a–c* (Informations- und Dokumentationssystem des Bundessicherheitsdienstes; Art. 75 f. VE-PolAG). Als Inhalte des VE-PolAG sind diese Bestimmungen bereits der Prüfung im Rahmen des oben erwähnten Vernehmlassungsverfahrens unterzogen worden. Dessen Ergebnis verlangte keine Anpassungen an den genannten Bestimmungen,[41] weshalb diese weitgehend unverändert aus dem VE-PolAG in die vorliegende BWIS-Revision übernommen werden.

Der Grundsatz der Einheit der Materie einer Vorlage verlangt, dass diese sachliche Geschlossenheit aufweist, ihre thematischen Teilbereiche also untereinander in einem klaren Sachzusammenhang stehen. Diese Anforderung ist erfüllt. Mit seinem neuen Geltungsbereich steht das BWIS zwar nicht in einem unmittelbaren Zusammenhang mit dem Gegenstand des Nachrichtendienstgesetzes, jedoch aber in einem weiter gefassten inneren sachlichen Zusammenhang: Beide – die nachrichtendienstlichen Aufgaben und Befugnisse des Bundes wie dessen begrenzte sicherheitspolizeiliche Aufgaben im verbleibenden BWIS – dienen dem übergeordneten Ziel der Wahrung der inneren Sicherheit im Kompetenzbereich des Bundes. Sicherheitspolizeiliche Funktionen werden im Übrigen von fedpol auch ausserhalb des oben genannten Aufgabenbereichs (Schutz von Personen und Gebäuden des Bundes sowie völkerrechtlich geschützter Personen) wahrgenommen. So kann sich die Bundeskriminalpolizei (BKP) im Rahmen der Erfüllung ihrer Aufgaben, etwa anlässlich der Verhaftung gewaltbereiter Personen, veranlasst sehen, ihre eigenen Ermittler und die zuständigen Staatsanwälte, aber auch unbeteiligte Drittpersonen (Passanten, Wohnungsnachbarn etc.) vor Gefahren zu schützen. Im direkten Zusammenhang mit dem Vollzug einer strafprozessualen Zwangsmassnahme ist folglich auch die BKP flankierend sicherheitspolizeilich tätig (Gefahrenabwehr). Dieser sicherheitspolizeilichen Funktion der BKP kommt innerhalb von deren Aufgabenbereich jedoch keine eigenständige, d.h. von einem konkreten kriminalpolizeilichen Auftrag unabhängige Bedeutung zu. Diese Funktion liegt auch ausserhalb der Regelungsmaterie «innere Sicherheit» und ist folglich nicht Gegenstand der vorliegenden BWIS-Teilrevision.

Art. 2 Aufgaben

Die Neuformulierung dieser Bestimmung wiederspiegelt den Umstand, dass sich das BWIS neu auf die Regelung von Aufgaben von fedpol beschränkt:

41 Vgl. den Bericht über das Ergebnis des Vernehmlassungsverfahrens zum Vorentwurf des Bundesgesetzes über die polizeilichen Aufgaben des Bundes, Bundesamt für Polizei, Oktober 2010, S. 24 (zu Art. 31 und 32 VE-PolAG) sowie S. 28 (zu Art. 75 f. VE-PolAG).

Abs. 1: Die nachrichtendienstliche Tätigkeit in den Bereichen Terrorismus und verbotener Nachrichtendienst sowie verbotener Handel mit Waffen und Technologietransfer sind neu im NDG geregelt (vgl. Art. 6 Abs. 1 NDG). «Massnahmen nach diesem Gesetz», also dem BWIS, sind neu einzig noch solche «polizeilicher» Natur. Um welche Massnahmenbereiche es sich im Einzelnen handelt, wird in Absatz 2 aufgeführt. Die *Absätze 2 und 3* des geltenden BWIS können ganz aufgehoben werden, da sie Inhalte betreffen, die neu im NDG geregelt sind. Der geltende Absatz 4 wird damit neu zu Absatz 2.

Abs. 2: Die periodische Beurteilung der Bedrohungslage und die Bearbeitung von Informationen über die innere und äussere Sicherheit (Art. 2 Abs. 4 Bst. a bzw. b des geltenden BWIS) sind in der Aufzählung der vorbeugenden polizeilichen Aufgaben nicht mehr enthalten, da diese Aufgaben neu im NDG geregelt sind. Die verbleibenden vier Aufgabenbereiche werden unverändert übernommen. Sie werden ergänzt durch einen neu aufgenommenen Buchstaben d (Beschlagnahme gefährlicher Gegenstände).

Art. 3 Schranken

Die generelle Regelung zu den inhaltlichen Schranken der Informationsbearbeitung im Zusammenhang mit nachrichtendienstlicher Informationsbeschaffung und Analyse findet sich neu im NDG (vgl. Art. 5 Abs. 5 und 6 NDG). Die im BWIS verbleibenden Bereiche der Informationsbearbeitung benötigen keine allgemeine Normierung inhaltlicher Schranken, da sie diesbezüglich über spezielle Regelungen verfügen (vgl. Art. 20 Abs. 1 letzter Satz für den Bereich der Personensicherheitsüberprüfungen sowie neu Art. 23*b* Abs. 3 für das Informationssystem des Bundessicherheitsdienstes [BSD]). Die Bestimmung kann entsprechend aufgehoben werden.

Art. 5 Aufgabenerfüllung durch den Bund

Grundlage für fedpol bei der Festlegung des Schutzniveaus für ausländische diplomatische und konsularische Vertretungen ist das entsprechende Leitbild des Bundesrates. Dieser Schutzauftrag ist gestützt auf die verfassungsrechtliche Kompetenzaufteilung im Bereich der inneren Sicherheit primär Sache der Kantone, während der Bund eine beratende und koordinierende Funktion ausübt (Bericht des Bundesrates vom 2. März 2012[42] in Erfüllung des Postulats Malama 10.3045 vom 3. März 2010 «Innere Sicherheit. Klärung der Kompetenzen»).

Die Absätze 2 und 3 in Artikel 5 des geltenden BWIS regeln Inhalte, die neu im NDG normiert sind (vgl. Art. 9 und 11 NDG). Sie erscheinen deshalb in der revidierten Fassung des BWIS nicht mehr.

Art. 5a

Der Inhalt dieser Norm wird im NDG geregelt, weshalb sie im BWIS aufzuheben ist.

42 BBl **2012** 4459, hier 4504, Ziff. 2.3.2.2.1.2

Art. 6 Abs. 1

Der Wortlaut der Norm wird dahingehend an den neuen Inhalt des BWIS angepasst, dass als Zusammenarbeitspartner nur noch fedpol festgelegt wird.

Art. 7–9

Diese Normen regeln spezifische NDB-Aufgaben, weshalb sie im BWIS aufzuheben sind.

Art. 10 Informationspflichten von fedpol

Der Wortlaut der Norm wird dahingehend an den neuen Inhalt des BWIS angepasst, dass fedpol als alleiniger Adressat der Informationspflicht genannt wird.

Art. 10a–13d

Diese Normen regeln spezifische NDB-Aufgaben, weshalb sie im BWIS aufzuheben sind.

Art. 13e Abs. 2

Die einzige Änderung gegenüber der geltenden Fassung dieser Norm besteht darin, dass der NDB, da in der vorliegenden Neufassung des BWIS hier erstmals genannt, in voller Behördenbezeichnung einschliesslich seiner Abkürzung eingeführt wird.

Art. 13f Beschlagnahme gefährlicher Gegenstände

Gemäss Artikel 28*a* des Waffengesetzes vom 20. Juni 1997[43] (WG) ist das Tragen gefährlicher Gegenstände an öffentlich zugänglichen Orten und das Mitführen solcher Gegenstände in Fahrzeugen verboten, wenn nicht glaubhaft gemacht werden kann, dass dies durch die bestimmungsgemässe Verwendung oder Wartung der Gegenstände gerechtfertigt ist und der Eindruck erweckt wird, dass die Gegenstände missbräuchlich eingesetzt werden sollen, insbesondere, um damit Personen einzuschüchtern, zu bedrohen oder zu verletzen. Als solche gefährliche Gegenstände gelten gemäss Artikel 4 Absatz 6 WG Gegenstände wie Werkzeuge, Haushalt- und Sportgeräte, die sich zur Bedrohung oder Verletzung von Menschen eignen. Taschenmesser, wie etwa das Schweizer Armeetaschenmesser und vergleichbare Produkte, gelten hingegen nicht als gefährliche Gegenstände. Nach Artikel 31 Absatz 1 Buchstabe c WG beschlagnahmt die zuständige Behörde gefährliche Gegenstände, die missbräuchlich getragen werden; wenn die Voraussetzungen gegeben sind, kann sie die beschlagnahmten Gegenstände definitiv einziehen (Art. 31 Abs. 3 WG). Laut Artikel 38 Absatz 1 WG vollziehen die Kantone das Gesetz, soweit nicht der Bund als zuständig erklärt wird.

Mit *Artikel 13f* soll fedpol in seinem Zuständigkeitsbereich neu befugt werden, derartige gefährliche Gegenstände zu beschlagnahmen. Im Rahmen des Schutzes von Behörden und Gebäuden des Bundes ist es für fedpol unerlässlich, diese gefähr-

43 SR **514.54**

lichen Gegenstände selbstständig beschlagnahmen und definitiv einziehen zu können. Ebenso muss fedpol bei der Wahrnehmung kriminalpolizeilicher Aufgaben die Sicherheit der involvierten Personen gewährleisten und Einschüchterungen oder Bedrohungen unmittelbar verhindern können.

Art. 14 Abs. 1

Die Änderung gegenüber dem geltenden Wortlaut dieser Norm besteht darin, dass als ihr Adressat seitens des Bundes – dem neuen Inhalt des BWIS entsprechend – einzig fedpol vorgesehen ist und nicht mehr generell «die Sicherheitsorgane des Bundes».

Art. 14a–18

Diese Normen regeln spezifische NDB-Aufgaben, weshalb sie im BWIS aufzuheben sind.

Art. 21 Abs. 2

Diese Änderung ist rein gesetzestechnischer Natur.

Art. 23 Abs. 1 Bst. a und c und 3bis

Abs. 1 Bst. a und c: Die Neufassung dieser Norm ist in zweifacher Hinsicht gegenüber dem geltenden Wortlaut präzisiert: Es wird klargestellt, dass grundsätzlich nur diejenigen Personen des Bundes schutzberechtigt sind, die eine Funktion im öffentlichen Interesse ausüben wie eidgenössische Parlamentarierinnen und Parlamentarier, Magistratspersonen sowie gewisse Angestellte des Bundes. Diese Personen sind aktuell in der Verordnung über das Sicherheitswesen in Bundesverantwortung vom 27. Juni 2001[44] (VSB) bereits aufgeführt. Gleichzeitig müssen diese Personen aufgrund der von ihnen wahrgenommenen Funktion einer besonderen Gefährdungslage ausgesetzt sein, um einen Anspruch auf Schutzmassnahmen zu haben. Daraus resultiert auch die Dauer der Schutzmassnahmen: Diese werden grundsätzlich nur gewährt, solange die Person für die Eidgenossenschaft eine Funktion ausübt, die mit besonderen Risiken verbunden ist. Befindet sich z.B. eine der genannten Personen ausserhalb ihrer beruflichen Funktion aus rein privaten Gründen in einer Bedrohungs- oder Gefährdungssituation, so sind für ihren Schutz – wie für jede andere Bürgerin und jeden anderen Bürger – die kantonalen Polizeibehörden aufgrund ihrer umfassenden sicherheitspolizeilichen Kompetenz zuständig.

Artikel 23 Absatz 1 Buchstabe c des geltenden BWIS (Gebäude und Anlässe, bei denen andere Schutzdienste eingesetzt werden) ist bisher nie angewendet worden und soll deshalb aufgehoben werden.

Abs. 3bis: Neu soll die Polizei – der BSD von fedpol oder die gegebenenfalls zuständige Kantonspolizei – befugt werden, mit einer Person in direkten Kontakt zu treten, von der sie annehmen muss, dass sie ein ernsthaftes Risiko für zu schützende Personen oder Gebäude darstellt. Die Polizei wird diese Person bezüglich der konkreten Hinweise auf strafbare Handlungen zur Rede stellen und sie auf die strafrechtlichen Konsequenzen einer Tatausführung hinweisen mit dem Ziel, sie von einer Tatbege-

44 SR **120.72**

hung abzuhalten (sogenannte Gefährderansprache). Die betroffene Person soll sich klar werden, mit welchen polizeilichen oder verwaltungsrechtlichen Massnahmen sie je nach Fehlverhalten zu rechnen hat. Erfahrungen aus Deutschland wie auch im Kanton Zürich im Bereich der häuslichen Gewalt, aber auch mit Hooligans während der EURO 2008 haben gezeigt, dass sich potenzielle Gefahrenverursacherinnen und -verursacher im direkten Gespräch mit der Polizei von einem deliktischen Vorhaben durchaus abbringen lassen. Bei der Gefährder–ansprache handelt es sich um eine Massnahme nicht formeller Natur. Die Massnahme wird im Informations- und Dokumentationssystem nach Artikel 23*a* vermerkt. Nachteilige Wirkungen auf die betroffene Person gehen von ihr nicht aus, und es erfolgt keine Mitteilung an andere Behörden oder Register.

Art. 23a Informations- und Dokumentationssystem

Abs. 1: Da der BSD auch Personendaten bearbeitet, setzt diese Datenbearbeitung gemäss Artikel 17 Absatz 2 DSG eine formellgesetzliche Grundlage voraus. Aktuell stützt sich die Informationsbearbeitung des BSD zur Wahrnehmung seines Schutzauftrags nach dem 5. Abschnitt des BWIS auf Artikel 3 Absatz 4 BWIS. Artikel 13 VSB führt die Gesetzesnorm näher aus. Ursprünglich war vorgesehen, eine neue, formellgesetzliche Grundlage in die Revisionsvorlage BWIS II aufzunehmen. Nachdem diese Vorlage im August 2005 vom EJPD zur Überarbeitung an fedpol zurückgewiesen worden war, wurde beschlossen, die geplante Neuregelung in das PolAG aufzunehmen. Mit Einstellung dieses Gesetzgebungsvorhabens soll die Neuregelung nun in das BWIS aufgenommen werden.

Der VE-PolAG hatte für die Informationsbearbeitung des BSD im Aufgabenbereich nach Artikel 22 Absatz 1 BWIS die zwei eigenständigen Informationssysteme «Ereignistabelle» und «BEDRO» vorgesehen (Art. 75 und 76 VE-PolAG). In der Vernehmlassung wurde bemängelt, dass die inhaltliche Abgrenzung zwischen den beiden Informationssystemen nicht gänzlich klar sei. Diese Kritik aufnehmend, werden die beiden heute getrennt geführten Informationssysteme neu zu *einem* umfassenden System zusammengelegt. Dieses Informationssystem ist Gegenstand der neuen Artikels 23*a* ff. Dass der zuständige Dienst von fedpol befugt ist, die erforderlichen Informationen zu beschaffen, ergibt sich bereits aus dem vorangehenden, allgemein formulierten Artikel 14 Absatz 1. Der vorliegende Artikel 23*a* schafft die geforderte spezielle formellgesetzliche Grundlage für das elektronische Informationssystem des BSD.

Abs. 2: Zur Erfüllung seines Schutzauftrags benötigt und bearbeitet fedpol Informationen einerseits zu sicherheitsrelevanten Ereignissen und andererseits zu damit verbundenen Personen. Ereignisse können Rückschlüsse auf die Gefährdung von Personen oder Gebäuden ermöglichen. Diese Ereignisse sind zu dokumentieren, um über die Tagesaktualität hinaus analysiert und in ihren grösseren Zusammenhängen situiert werden zu können. Die Informationen zu diesen Ereignissen stammen zu rund neunzig Prozent aus öffentlich zugänglichen Quellen. Der Kreis der mit den sicherheitsrelevanten Ereignissen verbundenen Personen umfasst zwei grundsätzlich verschiedene Kategorien von Personen: einerseits die von fedpol zu schützenden Personen und andererseits die potenziellen Urheber von Gefahren für Personen und Einrichtungen. Voraussetzung für die Aufnahme einer bestimmten Person in das Informationssystem ist, dass aufgrund konkreter Hinweise angenommen werden muss, dass von ihr eine Gefahr für bestimmte Personen und Gebäude ausgeht.

Art. 23b Daten, Datenkategorien und Schranken der Datenbearbeitung

Abs. 1: Im Informationssystem werden Daten aus ganz unterschiedlichen Quellen erfasst und bearbeitet. Am Anfang der Datenerfassung steht häufig ein Drohschreiben. Dieses ist in der Mehrzahl der Fälle anonym abgefasst. Um die Gefährlichkeit einer Person abschätzen zu können, ist es wichtig zu wissen, in welchem Grad eine Person gewaltbereit ist, wie sich ihre Gewaltbereitschaft in der Vergangenheit entwickelt hat und ob sie bereits wegen Gewaltdelikten verurteilt worden ist. Zur Abklärung der Identität der drohenden Person sowie der Beurteilung ihrer Gefährlichkeit müssen die notwendigen Informationen aus verschiedenen Quellen zusammengetragen werden. Der Grossteil der Informationen stammt auch hier aus öffentlich zugänglichen Quellen.

Abs. 3: Die Bestimmung legt die inhaltlichen Schranken der Informationsbearbeitung fest. Der Wortlaut ist aus Artikel 3 Absatz 1 des geltenden BWIS übernommen (der seinerseits, wie weiter oben erläutert, aufgehoben wird). Für nähere Ausführungen zur vorliegenden Norm kann auf die Erläuterungen zum inhaltlich entsprechenden Artikel 5 Absatz 5 und 6 NDG verwiesen werden.

Art. 23c Zugriffsrechte und Datenweitergabe

Der Datenzugriff ist differenziert geregelt: Nur bestimmte Organisationseinheiten von fedpol, nämlich diejenigen Stellen, die sich mit der Gefährdungsbeurteilung, dem Personenschutz oder dem Staatsschutz befassen, verfügen über einen direkten Online-Zugriff (*Abs. 1*). Den in *Absatz 2* aufgezählten Stellen können Daten einzelfallweise bekannt gegeben werden. So müssen z.B. die Mitarbeiterinnen und Mitarbeiter, die den Zugang zu den einzelnen Amtssitzen der Bundesräte kontrollieren, informiert werden können, wenn eine bestimmte Person für den sich im Gebäude aufhaltenden Bundesrat eine Gefahr darstellt. Zu diesen Informationen gehören neben den Personalien und einer Fotografie zur Identifikation der Person gewöhnlich auch Angaben über spezifische Persönlichkeitsstrukturen, etwa ihre Gewaltbereitschaft. Derartige Angaben dürfen auch zum Schutz von völkerrechtlich geschützten Personen in der Schweiz weiter gegeben werden. So muss z.B. eine ausländische Vertretung in unserem Land über Personen informiert werden, die für ihre Geschäftsträgerinnen und -träger ein Sicherheitsrisiko darstellen. Desgleichen müssen auch private Sicherheitsorganisationen, die z.B. im Auftrag von fedpol ein Gebäude bewachen, zur Erfüllung ihres Schutzauftrags derartige Informationen erhalten dürfen.

Art. 25–27

Der Regelungsinhalt dieser Bestimmungen befindet sich neu im NDG, weshalb sie im BWIS aufzuheben sind.

Art. 28 Abs. 1

Die Regelung der Abgeltung für Leistungen der Kantone im Rahmen der nachrichtendienstlichen Informationsbeschaffung findet sich neu in Artikel 81 Absatz 5, weshalb die entsprechende Norm im BWIS aufgehoben werden kann.

Bundesgesetz vom 20. Juni 2003[45] über das Informationssystem für den Ausländer- und den Asylbereich

Art. 9 Abs. 1 Bst. c und l sowie Abs. 2 Bst. c und k

In Artikel 9 Absatz 1 Buchstabe c (Zugriff via Abrufverfahren) sind heute die für die innere Sicherheit zuständigen Bundesbehörden erwähnt. Der Online-Zugriff auf das Informationssystem des Bundesamts für Migration (BFM) ist jedoch für den NDB auf die Prüfung von Fernhaltemassnahmen beschränkt, was nicht dem gesamten Aufgabenspektrum des NDB entspricht. So wirkt der NDB an zahlreichen Verfahren des Ausländer- und Asylbereichs mit, um mögliche Gefährdungen der inneren oder äusseren Sicherheit zu beurteilen. Deshalb wird vorgeschlagen, die Voraussetzungen für den Online-Zugriff entsprechend den gesetzlichen Aufgaben des NDB abzubilden und gleichzeitig in einem separaten Buchstaben von Artikel 9 Absatz 1 zu regeln. Die Vorbehalte von Gefährdungen der inneren oder äusseren Sicherheit sind im Ausländergesetz vom 16. Dezember 2005[46] und im Asylgesetz vom 26. Juni 1998[47] in zahlreichen Bestimmungen enthalten, weshalb hier der Gesetzestext auf einzelne Erwähnungen verzichtet.

Das gleiche gilt analog für Absatz 2 Buchstaben c und k.

Verwaltungsgerichtsgesetz vom 17. Juni 2005[48]

Art. 23 Abs. 2 und 36b

In Artikel 23 Absatz 2 Buchstabe b wird die Zuständigkeit der Präsidentin oder des Präsidenten der zuständigen Abteilung des Bundesverwaltungsgerichts für das Genehmigungsverfahren betreffend die genehmigungspflichtigen Beschaffungsmassnahmen und betreffend die Kabelaufklärung eingeführt.

Artikel 36*b* sieht demgegenüber die grundsätzliche Zuständigkeit des Bundesverwaltungsgerichts für die Genehmigung von Beschaffungsmassnahmen des NDB vor.

Art. 33 Bst. b Ziff. 4

Die Beschwerde gegen Verfügungen des Bundesrates über Tätigkeitsverbote (Art. 72) muss explizit vorgesehen werden, da sie bisher in der abschliessenden Aufzählung nach Artikel 33 Buchstabe b des Verwaltungsgerichtsgesetzes nicht enthalten ist.

45 SR **142.51**
46 SR **142.20**
47 SR **142.31**
48 SR **173.32**

Zivilgesetzbuch[49]

Art. 43a Abs. 4 Ziff. 5

Mit der Ergänzung in Artikel 43*a* Absatz 4 ZGB soll dem NDB der Zugriff auf das System Infostar (Zivilstandsregister) zum Zwecke der Identifizierung von Personen und deren gegenwärtigen und allenfalls früheren Aufenthalts ermöglicht werden. Der Bundesrat wird aber den Online-Zugriff des NDB auf Infostar in der Verordnung näher zu regeln haben (z.B. dessen Umfang). Die Nummerierung berücksichtigt die laufende Revision dieses Artikels, die zusätzliche Zugriffe anderer Stellen schaffen wird. Die Zugriffe des NDB sollen über analoge Schnittstellen erfolgen, die bereits von anderen Stellen des Bundes und der Kantone genutzt werden.

Strafgesetzbuch[50]

Art. 317bis Abs. 1 und 2

Der Hinweis auf das BWIS wird durch denjenigen auf das Nachrichtendienstgesetz ersetzt.

Art. 365 Abs. 2 Bst. r–u

Neu werden hier die Aufgaben des NDB aufgeführt, für deren Vollzug der NDB den Zugriff auf das automatisierte Strafregister (VOSTRA) benötigt. Diese Zugriffe bestehen heute schon in Anwendung der Ausnahmeregelung von Artikel 367 Absatz 3 StGB in Verbindung mit Artikel 21 Absatz 4 der VOSTRA-Verordnung vom 29. September 2006[51]. Dies gilt aber nur bis zum Inkrafttreten einer formellgesetzlichen Grundlage, die nun bei der neuen Gesetzgebung über den Nachrichtendienst geschaffen werden soll. Die Zugriffszwecke für den NDB werden dabei präzisiert und mit den nötigen Querverweisen auf das NDG versehen.

Art. 367 Abs. 2 Bst. m und Abs. 4

Zur formellrechtlichen Zugangsregelung gehört auch die Erwähnung des NDB in Artikel 367 StGB. In dieser Bestimmung sind die Behörden genannt, welche im Abrufverfahren online Zugang zu VOSTRA erhalten. Der NDB benötigt für die Erfüllung seiner gesetzlichen Aufgaben nicht nur Kenntnis von erfolgten Strafurteilen (vgl. Art. 367 Abs. 2 Bst. m; inkl. Freisprüche mit gerichtlichen Massnahmen), sondern auch von allfällig hängigen Strafverfahren (vgl. Art. 367 Abs. 4). Dies dient zum einen nicht nur der Verhinderung von Überschneidungen nachrichtendienstlicher Aktivitäten mit solchen der Strafverfolgungsorgane, sondern auch der korrekten Auskunftserteilung bei Unbedenklichkeitsabklärungen nach Artikel 12 Absatz 1 Buchstabe d NDG für ausländische Sicherheitsbehörden. Für die Absprache über die Weiterleitung von Auskünften über hängige Strafverfahren wird sich der NDB wie bisher mit der zuständigen Strafverfolgungsbehörde in Verbindung setzen, um negative Auswirkungen auf laufende Ermittlungen zu vermeiden.

49 SR **210**
50 SR **311.0**
51 SR **331**

Strafprozessordnung[52]

Die Änderung der Strafprozessordnung betrifft nur den französischen Text.

Bundesgesetz vom 13. Juni 2008[53] über die polizeilichen Informationssysteme des Bundes

Art. 15 Abs. 3 Bst. k und 4 Bst. i

Das NDG führt im Bereich der Zugriffe auf die polizeilichen Informationssysteme lediglich die Rechtsgrundlagen für schon heute bestehende Zugriffe nach (Art. 15 BPI, Automatisiertes Polizeifahndungssystem) und verankert die Möglichkeit zu Personen- und Sachfahndungsausschreibungen nach Artikel 16 NDG. Zugriff auf Daten werden nicht sämtliche Mitarbeiterinnen und Mitarbeiter des NDB haben, sondern nur diejenigen, die ihn für die Erfüllung der gesetzlich vorgesehenen Aufgaben benötigen. Der Bundesrat wird wie üblich in den Ausführungsverordnungen den Kreis der zugriffsberechtigten Mitarbeiterinnen und Mitarbeiter des NDB und den Umfang ihrer Zugriffe näher regeln. Die Verweise auf das BWIS werden durch solche auf die massgeblichen Normen des NDG ersetzt

Abs. 16 Abs. 9

Der Verweis auf das BWIS wird durch einen solchen auf die massgeblichen Normen des NDG ersetzt.

Militärgesetz vom 3. Februar 1995[54]

Art. 99 Abs. 1bis, 1^{quater} und 3bis

In Artikel 99 Absatz 1bis wird die neue gesetzliche Grundlage für die Funkaufklärung des Nachrichtendienstes der Armee verankert. Bisher bezog sich der entsprechende Verweis in Artikel 99 Absatz 1bis auf Artikel 4*a* ZNDG.

Absatz 1^{quater} stellt dem Nachrichtendienst der Armee dasselbe Mittel für die Beobachtung aus der Luft zu Verfügung wie dem NDB (Art. 14) und nimmt auch dessen Vorkehren zum Schutz der Privatsphäre auf.

Absatz 3bis entspricht der Bestimmung von Artikel 68 Absatz 2 NDG.

52 SR **312.0**
53 SR **361**
54 SR **510.10**

Bundesgesetz vom 3. Oktober 2008[55] über die militärischen Informationssysteme

Art. 16 Abs. 1 Bst. h

Neu wird vorgesehen, dass der NDB Online-Zugriff auf die PISA-Datenbank hat, damit er mögliche Bedrohungen für die Sicherheit der Armee durch Personen feststellen kann, die beispielsweise gewalttätig-extremistischen Gruppen angehören und in der Armee eingeteilt sind. So soll verhindert werden, dass gewaltorientierte Personen einerseits die Sicherheit der Armee gefährden, andererseits aber durch die Armee in der Handhabung von Waffen und Sprengstoffen und der Anwendung von Kampfverfahren ausgebildet werden.

Kernenergiegesetz vom 21. März 2003[56]

Art. 101 Abs. 3

Die Zentralstelle ATOM, um die es hier geht, ist dem NDB unterstellt. Aufgabe der Zentralstelle ist die Beschaffung und Bearbeitung von Daten, die für den Vollzug des Kernenergiegesetzes, die Deliktsverhütung und die Strafverfolgung erforderlich sind. In der Praxis hat sich gezeigt, dass es notwendig ist, den Tätigkeitsbereich der Zentralstelle auf den Bereich des Strahlenschutzgesetzes vom 22. März 1991[57] auszudehnen, der mit demjenigen des Kernenergiegesetzes eng verwandt ist. So können Abgrenzungsfragen über die Art radioaktiver Substanzen vermieden werden (spaltbares und nicht spaltbares Material), die zwar für deren Zuordnung zum Geltungsbereich der beiden Gesetze massgeblich, in der nachrichtendienstlichen Praxis aber nicht relevant sind, oder die beispielsweise bei der Aufnahme der Bearbeitung eines Falles von Atomschmuggel noch nicht beurteilt werden können.

Strassenverkehrsgesetz vom 19. Dezember 1958[58]

Art. 104c Abs. 5 Bst. c

Mit der Anpassung von Artikel 104*c* Absatz 5 soll der NDB Online-Zugriff auf das Fahrberechtigungsregister erhalten. Dieser Zugriff ist notwendig zur Feststellung der Fahrberechtigung von Personen, ohne die die Durchführung nachrichtendienstlicher Massnahmen wie Observationen nur ungenügend vorbereitet werden könnten.

55 SR **510.91**
56 SR **732.1**
57 SR **814.50**
58 SR **741.01**

Bundesgesetz vom 6. Oktober 2000[59] betreffend die Überwachung des Post- und Fernmeldeverkehrs

Dieses Gesetz wird derzeit einer Totalrevision unterzogen, die die Regelungen der Überwachung des Post-und Fernmeldeverkehrs (BÜPF) den neuen Bedürfnissen anpassen wird.[60] In diesem Rahmen sind weiterhin nur Überwachungen zur Strafverfolgung und zu eng umschriebenen polizeilichen Zwecken vorgesehen. Mit dem NDG wird der Zweck der Überwachung auf den nachrichtendienstlichen Bereich ausgedehnt, was entsprechend im BÜPF verankert werden muss.

Nach den Grundsätzen der Gesetzgebungstätigkeit kann eine Botschaft jedoch nur einen bestehenden Gesetzestext ändern. Deshalb nimmt die Botschaft des NDG in den Änderungen anderer Erlasse Bezug auf das bestehende BÜPF, während die Abstimmung mit der Totalrevision im Zug der parlamentarischen Beratung von NDG und BÜPF und gegebenenfalls der Inkraftsetzung durch den Bundesrat erfolgen muss.

Es folgen deshalb die Erläuterungen der Änderungen, die notwendig sind, um das bestehende BÜPF um Bestimmungen zur Überwachung für nachrichtendienstliche Zwecke zu erweitern.

Art. 1 Abs. 1 Bst. d

Der NDB kann neu Überwachungen des Post- und Fernmeldeverkehrs anordnen (Art. 25 Abs. 1 Bst. a–d). Die Durchführung dieser Massnahmen soll nach dem Verfahren gemäss BÜPF und über den dafür zuständigen Dienst ÜPF im EJPD erfolgen. Zu diesem Zweck muss der NDB neu zusätzlich als anordnende Stelle im BÜPF verankert werden.

Art. 11 Abs. 1 Bst. a und 13 Abs. 1 Bst. a

In diesen beiden Bestimmungen wird neu auch der NDB als berechtigte Stelle für die Erteilung von Überwachungsaufträgen genannt. Es handelt sich hier um das Korrelat zur Befugnis des NDB nach Artikel 25 Absatz 1 Buchstaben a–d NDG, den Post- und Fernmeldeverkehr einer Person überwachen zu lassen.

Art. 14 Abs. 2bis

Hier wurde lediglich der Verweis auf das BWIS ersetzt durch denjenigen auf das neue NDG.

59 SR **780.1**
60 BBl **2013** 2683

Koordination mit der Totalrevision des BÜPF

Es folgt eine Übersicht über die notwendigen Änderungen im totalrevidierten Entwurf des BÜPF[61], gemäss Botschaft vom 27. Februar 2013[62], unter Vorbehalt der Beratungen und der Beschlüsse der eidgenössischen Räte. Die Bestimmungen entsprechen in den Formulierungen, Inhalt und Detaillierungsgrad dem Entwurf des BÜPF.

Ingress

gestützt auf die Artikel *57 Absatz 2*, 92 Absatz 1 und 123 Absatz 1 der Bundesverfassung[63],
nach Einsicht in die Botschaft des Bundesrates vom 27. Februar 2013[64],

Art. 1 Abs. 1 Bst. e

1 Dieses Gesetz gilt für die Überwachung des Post- und Fernmeldeverkehrs, die angeordnet und durchgeführt wird:

e. im Rahmen des Vollzugs des Nachrichtendienstgesetzes (NDG) vom …[65]

Art. 5 Abs. 1

1 Das EJPD kann ein beratendes Organ einsetzen, dem Vertreterinnen und Vertreter des EJPD, des Dienstes, der Kantone, der Strafverfolgungsbehörden, des Nachrichtendienstes des Bundes (NDB) und der Anbieterinnen von Post- und Fernmeldedienstleistungen angehören.

Art. 10 Abs. 2bis

2bis Das Recht auf Auskunft über die Daten, welche beim Vollzug des NDG gesammelt wurden, richten sich nach dem NDG.

Art. 11 Abs. 3bis

3bis Die im Rahmen des Vollzugs des NDG gesammelten Daten sind im Verarbeitungssystem so lange aufzubewahren, wie es für das verfolgte Ziel erforderlich ist, längstens aber bis 30 Jahre nach Abschluss der Überwachung.

Art. 14a Schnittstelle zum Informationssystem des NDB

1 Die im Verarbeitungssystem enthaltenen Daten können im Abrufverfahren in das Informationssystem nach Artikel 56 des NDG kopiert werden, sofern:

a. das anwendbare Recht die Datenbearbeitung in diesem System erlaubt; und

b. sichergestellt ist, dass nur die mit der betreffenden Überwachungsmassnahme befassten Personen Zugriff auf die Daten haben.

61 BBl **2013** 2789
62 BBl **2013** 2683
63 SR **101**
64 BBl **2013** 2683
65 SR …

[2] Der Übermittlungsvorgang der Kopie kann nur von einer Person ausgelöst werden, die über Zugriffsrechte auf das Verarbeitungssystem nach diesem Gesetz und auf das betreffende Informationssystem nach dem NDG verfügt.

Art. 15 Abs. 1 Bst. d und Abs. 2 Bst. a

[1] Der Dienst erteilt ausschliesslich den folgenden Behörden auf Gesuch Auskünfte über die Daten nach Artikel 21 und 22, und dies nur zu den folgenden Zwecken:

d. dem Nachrichtendienst des Bundes: zwecks Erfüllung von Aufgaben nach dem NDG.

[2] Der Dienst erteilt den folgenden Behörden auf Gesuch Auskünfte über die Daten nach Artikel 21, und dies nur zu den folgenden Zwecken:

a. dem Nachrichtendienst des Bundes: zwecks Vollzug des NDG;

Art. 22a Auskünfte zur Identifikation von Personen bei Bedrohungen der inneren oder äusseren Sicherheit

Bestehen hinreichende Anhaltspunkte, dass eine Bedrohung der inneren oder äusseren Sicherheit über das Internet begangen wird oder worden ist, so sind die Anbieterinnen von Fernmeldediensten verpflichtet, dem Dienst alle Angaben zu liefern, welche die Identifikation der Urheberschaft oder Herkunft ermöglichen.

Ferner müsste Artikel 24 NDG für die Auskünfte über Fernmeldeanschlüsse neu auf Artikel 15 BÜPF (mit dem Datum der Totalrevision) verweisen.

Im totalrevidierten BÜPF sind die Überwachungsmassnahmen nicht mehr in gleicher Weise aufgeführt wie im gegenwärtigen Gesetz. Das NDG müsste deshalb zur Übernahme einer analogen Regelungsverteilung, wie sie zwischen BÜPF und Strafprozessordnung vorgesehen ist, wie folgt formuliert sein (die Erläuterungen entsprechen jenen in der Botschaft zum totalrevidierten BÜPF):

Art. 25 Abs. 1 Bst. a und a^{bis} (NDG)

[1] Die folgenden Beschaffungsmassnahmen sind genehmigungspflichtig:

a. Überwachungen des Postverkehrs und des Fernmeldeverkehrs und Verlangen von Randdaten des Postverkehrs und des Fernmeldeverkehrs gemäss dem Bundesgesetz vom …[66] betreffend die Überwachung des Post- und Fernmeldeverkehrs;

a^{bis}. Einsetzen von besonderen technischen Geräten zur Überwachung des Fernmeldeverkehrs, um Übermittlungen zu erfassen oder eine Person oder Sache zu identifizieren oder deren Standort zu ermitteln, wenn Überwachungen nach Buchstabe a erfolglos geblieben sind, aussichtslos wären oder unverhältnismässig erschwert würden und die fernmelderechtlichen Bewilligungen für die besonderen technischen Geräte vorliegen;

66 SR **780.1**

Fernmeldegesetz vom 30. April 1997[67]

Art. 34 Abs. 1ter und 1quater

Neu wird in Absatz 1ter auch der NDB erwähnt. Damit wird im FMG das erforderliche, formellgesetzliche Pendant zu Artikel 7 Absatz 1 Buchstabe d NDG geschaffen.

Zusammenfassender Hinweis zu den Bundesgesetzen nach den Ziffern 14–20:

Bei den Bundesgesetzen nach den Ziffern 14–20 wurden in den Artikeln zur Auskunftgabe lediglich formale Anpassungen vorgenommen. Es wird jeweils der Verweis auf das BWIS durch den Verweis auf das NDG ersetzt. Materiell ergeben sich keine Änderungen.

Ferner wird in einigen Gesetzen der mit BWIS II eingeführte Verweis auf die Erteilung von Auskünften an den NDB gestrichen, sofern es sich um die Auskunfterteilung «im Einzelfall auf schriftlich begründetes Gesuch hin» handelt. Dieser Verweis hat sich als unnötig erwiesen, weil die Auskunftgabe an den NDB jeweils bereits in einer anderen Bestimmung enthalten ist. Es erfolgt somit lediglich eine Korrektur eines gesetzgeberischen Versehens und keine Änderung der Rechtslage.

Bundesgesetz vom 19. Juni 1992[68] über die Militärversicherung

Art. 1a Abs. 1 Bst. q

Diese Bestimmung bildet das Pendant zu Artikel 35 Absatz 6 NDG, wonach die im Ausland eingesetzten Mitarbeitenden des NDB der Militärversicherung unterstellt sind. Diese Bestimmung soll auch im MVG als Quellerlass verankert werden.

Art. 95a Abs. 1 Bst. hbis und i Ziff. 8

Hier handelt es sich um die oben erwähnte formale Anpassung (Ersatz des Verweises auf das BWIS durch denjenigen auf das NDG).

3 Auswirkungen

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen

Die finanziellen Auswirkungen sind stark abhängig von der Art der Realisierung der einzelnen Massnahmen und der Häufigkeit, mit der diese zur Anwendung gelangen. Der Bundesrat rechnet damit, dass bei der heutigen Bedrohungslage solche Massnahmen in rund zehn Fällen pro Jahr zur Anwendung kommen, wobei pro Fall mehrere Massnahmen möglich sind.

67 SR **784.10**
68 SR **833.1**

Die Mittel und Systeme, welche bei der technischen Standortfeststellung im Ausland sowie bei der luft- und weltraumgestützten Beobachtung zum Einsatz kommen, sind bekannt und etabliert; ihre finanziellen Auswirkungen können daher gut beurteilt werden. Es fallen Beschaffungs- bzw. Investitionskosten von fünf bis sieben Millionen Franken sowie jährlich wiederkehrende Kosten von rund 800 000 Franken für die Instandhaltung und Anpassung dieser Systeme sowie Lizenzkosten an. Die Beschaffung und Finanzierung dieser Systeme erfolgt in der Regel über den Rüstungsablauf.

Bei den genehmigungspflichtigen Beschaffungsmassnahmen im Inland wie z.B. Standortfeststellungen, Überwachung von Nutz- und Verkehrsdaten bei Festnetz- und Mobiltelefonen oder etwa der Überwachung von Internetzugängen wird sich der NDB auf den zuständigen Dienst ÜPF abstützen. Hier wird bei der geschätzten Fallzahl mit einem jährlichen Gebührenanfall von rund 500 000 Franken gerechnet.

Für Übersetzungsarbeiten der aufgezeichneten Kommunikationen sind jährlich rund 800 000 Franken zu veranschlagen.

Die Kosten für die Entschädigung der Anbieterinnen bei der Kabelaufklärung (Art. 38 ff.) werden in Analogie zur Entschädigung der Fernmeldeüberwachung über den Dienst ÜPF auf ebenfalls rund 500 000 Franken pro Jahr geschätzt.

Bestimmte Technologien wie z.B. das Eindringen in besonders gesicherte Computersysteme sind noch wenig entwickelt. Zusammen mit dem Umstand, dass der Markt für diese Systeme vergleichsweise klein und volatil ist und zudem die technische Entwicklung auf diesem Gebiet rasch voranschreitet, können diese Systemkosten heute nur annähernd geschätzt werden.

Für die Ausrüstung der zusätzlichen Stellen sowie die Ausbildung der betroffenen Personen fallen Sachaufwände von rund 720 000 Franken (35 000 Franken pro Vollzeitstelle) an.

3.1.2 Personelle Auswirkungen

Bei der Umsetzung der neu vorgeschlagenen Beschaffungsmassnahmen soll, wo immer möglich auf den bestehenden Strukturen (NDB, Führungsunterstützungsbasis der Armee [FUB], Dienst ÜPF im EJPD) aufgebaut werden. Insgesamt werden aber 20,5 zusätzliche Stellen benötigt. Diese verteilen sich auf folgende neue Funktionen: Im NDB operative Technikerinnen und Techniker für die technische Betreuung der genehmigungspflichtigen Beschaffungsmassnahmen, Analytikerinnen und Analytiker für die operative Auswertung von Informationen, die mit genehmigungspflichtigen Massnahmen beschafft wurden, Juristinnen und Juristen für das Vorbereiten der Anträge, die Vollzugskontrolle und Berichterstattung im Zusammenhang mit genehmigungspflichtigen Beschaffungsmassnahmen; auch in der Qualitätssicherung der neuen Systeme und der Ansteuerung der Kabelaufklärung müssen Stellen geschaffen werden. Weitere Stellen werden benötigt für das Bundesverwaltungsgericht für das Genehmigungsverfahren für Beschaffungsmassnahmen, das Bundesarchiv für die Archivierung und das Zentrum Elektronische Operationen (ZEO) der FUB für den Testbetrieb der Kabelaufklärung. Diese 20,5 Stellen sollen gestaffelt besetzt werden (im ersten Jahr [1. Priorität] 12 Stellen, im zweiten Jahr [2. Priorität] 8,5 Stellen).

Die gegenüber dem heutigen Stand steigenden Anforderungen an die Datenhaltung werden grösstenteils durch die vorhandenen Ressourcen aufgefangen.

3.1.3 Andere Auswirkungen

Die Unterstützungsleistungen zugunsten Dritter sind ihrer Natur gemäss nicht planbar. Die Bereitstellung der notwendigen finanziellen und personellen Ressourcen muss fallweise mit dem Bedarfsträger bzw. dem Auftraggeber geregelt werden. Sie hängt unter anderem von den Möglichkeiten des NDB ab.

Ebenfalls nicht planbar sind Einsätze des NDB in besonderen Lagen zur Wahrung wesentlicher Landesinteressen nach Artikel 3. Hier werden ebenfalls keine zusätzlichen Stellen und Sachmittel auf Vorrat hin beantragt. Kann der NDB bei einem solchen Auftrag nicht auf bereits vorhandene Mittel, Ressourcen und Fachkenntnisse zurückgreifen, so müssen diese neu beantragt werden.

3.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Nach dem Konzept des Gesetzesentwurfs nimmt der NDB die nachrichtendienstlichen Aufgaben in Zusammenarbeit mit den kantonalen Vollzugsbehörden wahr.

An der bewährten Form der heutigen dezentralen Organisation und an der engen Zusammenarbeit mit den Kantonen wird festgehalten. Wie bisher sind für die innere Sicherheit ihrer Gebiete in erster Linie die Kantone zuständig. Soweit nach Verfassung und Gesetz der Bund für die innere Sicherheit verantwortlich ist, leisten ihm die Kantone Amts- und Rechtshilfe. Der NDB arbeitet eng mit der KKPKS und mit der KKJPD zusammen.

Bei bestimmten Bedrohungen sind grundsätzlich alle Behörden und Verwaltungseinheiten der Kantone nach dem Prinzip der Amtshilfe zur Auskunft verpflichtet. Die Auskünfte können vom NDB oder von den kantonalen Vollzugsbehörden eingeholt werden.

Neu führen die kantonalen Vollzugsbehörden im Anwendungsbereich dieses Gesetzesentwurfs keine eigenen Datensammlungen mehr. Dafür haben sie Zugriff auf die für die Erfüllung ihrer Aufgaben erforderlichen Informationen des NDB. Der Entwurf sieht für die kantonalen Vollzugsbehörden einen Zugriff mittels Abrufverfahren auf das System INDEX NDB vor. Dank diesem Zugriff können die Kantone u.a. die von ihnen erstellten Vorabklärungen und Berichte abrufen.

Die nachrichtendienstliche Kontrollinstanz des VBS kann in jenen Bereichen, in denen die kantonalen Vollzugsbehörden die Vorlage vollziehen, Kontrollen durchführen.

Bezüglich der parlamentarischen Aufsicht wird auf die Erläuterungen zu Artikel 77 verwiesen.

Der NDB trägt wie bisher zur Finanzierung der kantonalen Vollzugsbehörden bei.

3.3 Auswirkungen auf die Volkswirtschaft und auf die Gesellschaft

Die vorgeschlagenen Normen führen zu einer Stärkung der inneren und äusseren Sicherheit und damit zu einem noch besseren Schutz der Bevölkerung. Indirekt werden durch ein sicheres und gesellschaftlich stabiles Umfeld die wirtschaftlichen Rahmenbedingungen verbessert, was den Standort Schweiz stärkt.

3.4 Andere Auswirkungen

Die Vorlage setzt formal keine direkten internationalen Verpflichtungen um. Das internationale Ansehen der Schweiz kann sich jedoch nachhaltig verbessern, namentlich, weil die Schweiz ihren Willen demonstriert, den Terrorismus wirkungsvoll zu bekämpfen. Insbesondere die erweiterten Informationsbeschaffungsmassnahmen führen voraussichtlich zu einer besseren internationalen Zusammenarbeit.

4 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates

4.1 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Botschaft vom 25. Januar 2012[69] zur Legislaturplanung 2011–2015 und im Bundesbeschluss vom 15. Juni 2012[70] über die Legislaturplanung 2011–2015 angekündigt.

4.2 Verhältnis zu nationalen Strategien des Bundesrates

Am 25. März 2009 beschloss der Bundesrat die Zusammenführung des damaligen Inlandnachrichtendienstes mit dem Auslandnachrichtendienst zu einem neuen Bundesamt. Im sicherheitspolitischen Bericht des Bundesrates wird der NDB als Kompetenzzentrum für sämtliche nachrichtendienstliche Belange der inneren und äusseren Sicherheit positioniert und als sicherheitspolitisches Instrument verankert. Mit dem vorliegenden Gesetzesentwurf wird dieser Weg konsequent weiter beschritten, indem die massgebenden Normen einerseits in einem einzigen Erlass zusammengefasst und anderseits an neue Erfordernisse angepasst werden.

Besondere Beachtung finden die nationalen Strategien zum Schutz kritischer Infrastrukturen[71] und zum Schutz der Schweiz vor Cyber-Risiken[72]. Beide Strategien fordern eine aktive Rolle des Nachrichtendienstes zum frühzeitigen Erkennen und Verhindern von Angriffen auf kritische Infrastrukturen. Entsprechend wurde der Auftrag des NDB in Artikel 6 explizit ergänzt. Soweit die Angriffe auf kritische

69 BBl **2012** 481, hier 558 und 612
70 BBl **2012** 7155, hier 7159
71 www.bevoelkerungsschutz.admin.ch>Themen > Schutz kritischer Infrastrukturen > Publikationen SKI > Grundstrategie des Bundes zum Schutz Kritischer Infrastrukturen
72 www.isb.admin.ch > Themen > Cyber-Risiken NCS > Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS

Infrastrukturen mit IKT-Mitteln geführt werden, sollen sie auch aktiv unterbunden werden können (vgl. Art. 25 Abs. 1 Bst. d).

5 Rechtliche Aspekte

5.1 Verfassungs- und Gesetzmässigkeit

Nach den verfassungsrechtlichen Regeln der Kompetenzverteilung zwischen dem Bund und den Kantonen kann der Bund dann gesetzgeberisch tätig werden, wenn die Bundesverfassung ihm die notwendige Kompetenz zuweist. Wo keine solche Kompetenzzuweisung vorliegt, sind nach den allgemeinen Regeln die Kantone zuständig. (Art. 3 und 42 Abs. 1 BV).

Im Bereich der inneren und äusseren Sicherheit ist für die Frage, ob die Bundesverfassung dem Bund eine Gesetzgebungskompetenz zuweist, indessen nicht allein der Verfassungstext massgebend. Vielmehr fallen Kompetenzen, die sich aus der staatlichen Existenz der Eidgenossenschaft ergeben, auch dann in die Kompetenz des Bundes, wenn sie in der BV nicht ausdrücklich genannt werden (sogenannte inhärente Kompetenzen; vgl. BGE 117 IA 202, Erwägung 4a). So gilt es als inhärente Kompetenz des Bundes, im Inneren und im Äusseren die notwendigen Massnahmen zu seinem Schutz und zum Schutz seiner Organe und Institutionen zu treffen; der Bund hat den Bestand des gesamtschweizerischen Gemeinwesens zu gewährleisten und zu sichern und für die Abwehr von Gefahren zu sorgen, die dieses Gemeinwesen existenziell bedrohen. Die inhärente Kompetenz des Bundes im Bereich der inneren und äusseren Sicherheit schliesst auch Gesetzgebungsbefugnisse mit ein.

Im Bereich der äusseren Sicherheit verfügt der Bund zudem über eine allgemeine Kompetenz, die ebenfalls umfassende Rechtsetzungsbefugnisse beinhaltet. Dazu gehört unter anderem die Befugnis, Informationen über das Ausland zu beschaffen, die für die Einschätzung der sicherheitspolitischen Lage bedeutsam sein können. Soweit ein enger Bezug zu auswärtigen Angelegenheiten besteht, gilt Artikel 54 BV auch als Verfassungsgrundlage für innerstaatliche Akte.

Die Existenz von ungeschriebenem Verfassungsrecht gilt in der Verfassungslehre als gesichert. Nach geltender Rechtslage ist der Bund somit zur Gesetzgebung sowohl im Bereich des Staatsschutzes im Inland als auch im Bereich des Nachrichtendienstes im Ausland befugt. Für solche Bundeszuständigkeiten, die sich aus der Existenz und der Natur der Eidgenossenschaft ergeben und für die eine explizite Zuweisung einer Kompetenz an den Bund fehlt, wird nach neuer Praxis Artikel 173 Absatz 2 BV herangezogen. Im vorliegenden Kontext ist deshalb die Schaffung einer ausdrücklichen Verfassungsgrundlage für den Nachrichtendienst nicht zwingend erforderlich. Diese in der Vernehmlassung teilweise erhobene Forderung stützt sich unter anderem auch auf Erkenntnisse aus dem Bericht des Bundesrates in Erfüllung des Postulats Malama. Zwar wurde in diesem Bericht empfohlen, im Rahmen einer umfassenden Aktualisierung der verfassungsrechtlichen Kompetenzaufteilung zwischen Bund und Kantonen im Bereich der inneren Sicherheit auch eine explizite Verfassungsgrundlage für die Staatsschutztätigkeit des Bundes zu schaffen, doch verzichteten die eidgenössischen Räte in der Beratung des Berichts darauf, einen entsprechenden Auftrag an den Bundesrat zu formulieren. Der Bundesrat geht mit dem vorliegenden Gesetzesentwurf nicht über das hinaus, was verfassungsrechtlich

schon heute in der Zuständigkeit des Bundes liegt. Er kann sich dabei folglich auf eine ausreichende Verfassungsgrundlage stützen.

Schutz der Grundrechte für Personen in der Schweiz

Schwerwiegende Grundrechtseingriffe können im Rahmen dieser Vorlage bei den genehmigungspflichtigen Beschaffungsmassnahmen stattfinden (z.B. bei der Telefonabhörung oder bei Bild- und Tonaufnahmen in Privaträumen). Betroffen sind vor allem die Grundrechte auf Schutz der Privatsphäre (Art. 13 BV; Art. 8 EMRK) sowie je nach Sachlage weitere Garantien wie die persönliche Freiheit (Art. 10 Abs. 2 BV) und die Meinungs- und Informationsfreiheit (Art. 16 BV; Art. 10 EMRK). Genehmigungspflichtige Beschaffungsmassnahmen nach dem vorliegenden Gesetzesentwurf werden nur in der Schweiz durchgeführt.

Die im Entwurf enthaltenen genehmigungspflichtigen Beschaffungsmassnahmen tragen dem Erfordernis nach einer formellgesetzlichen Grundlage Rechnung, die auch dem Bestimmtheitsgebot genügt. Die vorgeschlagenen Regelungen erfüllen ferner die verfassungsmässigen Anforderungen der Verhältnismässigkeit und des Vorliegens eines genügenden öffentlichen Interesses.

Was die Natur der vorgesehenen Informationsbeschaffung betrifft, so sieht der Entwurf keine Massnahmen vor, die Eingriffe in die körperliche Integrität beinhalten, wie beispielsweise körperliche Untersuchungen oder die Anwendung körperlichen Zwangs. Solche Massnahmen sollen weiterhin Polizeibehörden vorbehalten bleiben, die zur Erfüllung ihrer Aufgaben polizeilichen Zwang oder polizeiliche Massnahmen einsetzen dürfen (vgl. Zwangsanwendungsgesetz vom 20. März 2008[73]).

Schliesslich enthält der Gesetzesentwurf (wie schon das BWIS) das grundsätzliche Verbot, in der Schweiz Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit zu sammeln. Es wird auf die Erläuterungen zu Artikel 5 Absatz 5 verwiesen.

Schutz der Grundrechte für Personen im Ausland

Die Beschaffung von Informationen im Ausland ist heikel, weil hier die Souveränität ausländischer Staaten und die Grundrechte von Personen im Ausland (z.B. die Wahrung der Privatsphäre) tangiert werden können.

Die Informationsbeschaffung im Ausland soll deshalb nur erfolgen, wenn die benötigten Informationen im Inland nicht beschafft werden können. Sie dient primär der Beurteilung und Abwehr von sicherheitspolitischen Bedrohungen für die Schweiz, z.B. in den Bereichen Terrorismus, Proliferation, und wird eingesetzt, wenn es darum geht, die Entwicklung von machtpolitischen Verhältnissen und Konflikten einzuschätzen.

Im Spannungsfeld zwischen den Sicherheitsinteressen der Schweiz und dem Schutz der Grundrechte von Personen im Ausland, müssen die Grundrechte stets berücksichtigt werden. Der NDB setzt dies um, indem ein allfälliger Grundrechtseingriff nicht in einem Missverhältnis zum erwarteten Informationsgewinn stehen darf.

Die gegenüber dem Inland weniger weit gehenden verfahrensmässigen Sicherungen betreffen vor allem die Beschaffungsmassnahmen im Sinne von Artikel 22 der

73 SR **364**

Vorlage. Gegen eine zum Inland analoge Genehmigungspflicht sprechen – abgesehen von den oben erwähnten grundsätzlichen Überlegungen – folgende Gründe:

- Für eine schweizerische Genehmigungsinstanz wäre es aufgrund der örtlichen Distanz schwierig oder sogar unmöglich, sich innert nützlicher Frist ein Bild von der Lage vor Ort zu machen und gestützt darauf einen sachgerechten Entscheid zu fällen.
- Die Genehmigung der schweizerischen Instanz würde an der Rechtswidrigkeit der Massnahme gegenüber dem ausländischen Recht nichts ändern.

Wenn Informationen über das Ausland dagegen im Inland beschafft werden, gilt der für die Schweiz gültige Grundrechtsschutz, insbesondere betreffend die genehmigungspflichtigen Beschaffungsmassnahmen. Davon ausgenommen ist das Eindringen in Computersysteme und -netzwerke, die sich im Ausland befinden (Art. 36).

Abgrenzung zur Tätigkeit der Polizei- und Strafverfolgungsbehörden

Nachrichtendienstliche Abklärungen bezwecken die Klärung, ob eine sicherheitspolitisch relevante Bedrohung der Schweiz vorliegt. Die Bedrohung kann sowohl durch ein Verhalten, das sich letztlich als nicht strafbar erweist, als auch durch strafbares Verhalten ausgelöst werden. Adressaten der nachrichtendienstlichen Abklärungsresultate sind primär die politischen Entscheidungsträger, d.h. die Exekutivorgane von Bund und Kantonen, damit diese rechtzeitig nach ihrem massgebenden Recht eingreifen können. Werden konkrete strafbare Handlungen aufgedeckt, so informiert der Nachrichtendienst auch die Strafverfolgungsbehörden.

Demgegenüber dient die Ermittlung bei der Strafverfolgung der Klärung eines Straftatverdachts bzw. einer individuellen Tatschuld und erfolgt und konzentriert sich auf die jeweiligen Tatbestandsmerkmale und nicht primär auf sicherheitspolitische Gesichtspunkte. Die Strafverfolgungsorgane bringen die Resultate ihrer Ermittlungen in gerichtliche Verfahren ein und nicht vor politische Instanzen. Sie verfolgen keine unmittelbaren sicherheitspolitischen Interessen, auch wenn die erfolgreiche Strafverfolgung auch Sicherheitsinteressen dient.

Die Abklärung von nachrichtendienstlichen Bedrohungslagen unterscheidet sich folglich von den Ermittlungen bei strafrechtlich relevantem Handeln nach dem StGB, und zwar in Bezug auf das auslösende Ereignis (hier Verdacht auf Bedrohung der Sicherheit der Schweiz, dort Verdacht auf Begehung einer konkreten Straftat), den Gegenstand der Abklärungen (hier Aufdecken von Absichten, Strukturen und Netzwerken, dort Nachweis strafbaren Verhaltens) und das damit verfolgte primäre Ziel (hier Schaffen einer Entscheidungsgrundlage für durch die Exekutive zu ergreifende Massnahmen, dort Klärung eines Straftatverdachts bzw. einer individuellen Tatschuld).

Berührungspunkte bestehen dort, wo sich in einem konkreten Einzelfall nachrichtendienstliche Abklärungen im Zusammenhang mit der Sicherheit der Schweiz mit Ermittlungen der Strafbehörden über strafrechtlich relevantes Verhalten überschneiden, weil die unter Straftatverdacht stehende Person oder die mutmassliche Straftat gleichzeitig Gegenstand präventiver Interessen ist. Dieselbe Person oder Tat kann somit gleichzeitige Abklärungen verursachen, dies jedoch unter grundlegend verschiedenen Blickwinkeln. Die jeweiligen Verfahren können sich deshalb teilweise ergänzen, aber nicht ersetzen. Das Nachrichtendienstgesetz ermöglicht die Koordination dieser Tätigkeiten durch die Regelung entsprechender Informationsflüsse und Absprachen.

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Im Völkerrecht besteht keine umfassende vertragliche Regelung betreffend zwischenstaatliche Spionage. Gemäss Völkergewohnheitsrecht werden Spionageaktivitäten in den zwischenstaatlichen Beziehungen in einem gewissen Ausmass toleriert. Der Spionage ausgesetzte Staaten stufen diese in der Regel nicht als völkerrechtswidrige Handlung, sondern als unfreundlichen Akt ein. Gleichzeitig behalten sich die meisten Staaten selbst explizit das Recht vor, im Ausland Spionage zu betreiben. Das fehlende generelle Verbot der zwischenstaatlichen Spionage im Völkerrecht hindert die Staaten nicht, in ihrem Landesrecht strafrechtliche Folgen für denjenigen vorzusehen, welcher die Tat der Spionage durchführt. Die meisten Staaten kennen wie die Schweiz derartige Strafbestimmungen in ihrem Landesrecht. Ebenso sieht das Landesrecht oftmals weitere Abwehrmassnahmen gegen ausländische Spionage vor.

Obwohl zwischenstaatliche Spionage daher an sich völkerrechtlich nicht verboten ist, kennt das Völkerrecht in Teilbereichen Normen, welche Spionageaktivitäten im Ausland beschränken können. So enthalten beispielsweise verschiedene Instrumente zum Schutz der Grund- und Menschenrechte oder auch die Wiener Konvention vom 18. April 1961[74] über diplomatische Beziehungen entsprechende Normen. Auch beim Handeln staatlicher Organe im Ausland ist grundsätzlich der Grund- und Menschenrechtsschutz zu akzeptieren. Gerade die Wiener Konvention wird indessen in der Praxis oft missachtet, sei es durch den Missbrauch der diplomatischen Vorrechte zur Spionage oder das Übergehen des diplomatischen Schutzes von Personen und Einrichtungen durch deren nachrichtendienstliche Ausforschung.

Zentral betroffen sind u.a. das Grundrecht auf Schutz der Privatsphäre (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II[75]). Berührt sein können, je nach Sachumständen, weitere Garantien, so die Grundrechte der Meinungs- und Informationsfreiheit (Art. 16 BV; Art. 10 EMRK; Art. 19 UNO-Pakt II), der Medienfreiheit (Art. 17 BV; Art. 10 EMRK), der Versammlungsfreiheit (Art. 22 BV; Art. 11 EMRK; Art. 21 UNO-Pakt II) und der Vereinigungsfreiheit (Art. 23 BV; Art. 11 EMRK; Art. 22 UNO-Pakt II), weiter etwa die persönliche Freiheit (Art. 10 Abs. 2 BV), die Religionsfreiheit (Art. 15 BV; Art. 9 EMRK; Art. 18 UNO-Pakt II), die Wirtschaftsfreiheit (Art. 27 BV) oder die Rechtsgleichheit (Art. 8 BV; Art. 2 und 26 UNO-Pakt II). Der Schutz der Privatsphäre (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II) kann im vorliegenden Kontext als eigentliches «Leitgrundrecht» betrachtet werden.

In diesem Zusammenhang ist auch zu beachten, dass Grundrechtseingriffe ab einer gewissen Schwere vor ihrer Anwendung ein gerichtliches (Bundesverwaltungsgericht) und politisches Genehmigungsverfahren durchlaufen müssen, sie nach Abschluss der Operation der betroffenen Person mitgeteilt werden müssen und auch nachträglich einer richterlichen Kontrolle (Bundesverwaltungsgericht mit Weiterzugsmöglichkeit an das Bundesgericht) zugeführt werden können. Daneben bestehen Auskunftsrechte (sei es nach DSG, sei es die Möglichkeit während der Dauer eines begründeten Geheimhaltungsinteresses durch Vermittlung des EDÖB bzw. des

74 SR **0.191.01**
75 SR **0.103.2;** Internationaler Pakt vom 16. Dezember 1966 über bürgerliche und politische Rechte

Bundesverwaltungsgerichts ein entsprechendes Ersuchen zu stellen), sodass wirksame Massnahmen im Sinne der EMRK gegen allfällige Missbräuche bestehen.

Die im Gesetzesentwurf vorgesehenen Tätigkeiten des NDB erfolgen damit völkerrechtskonform.

Besondere völkerrechtliche Fragen stellen sich, wenn im Ausland nicht nur aktiv nachrichtendienstlich Informationen gesammelt werden, sondern computergestützte Massnahmen ergriffen werden, um in Reaktion auf einen Cyber-Angriff aus dem Ausland den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Eine derartige umfassende völkerrechtliche Beurteilung wird der Bundesrat im Einzelfall vornehmen, wenn er über derartige Massnahmen entscheidet.

5.3 Erlassform

Nach Artikel 164 Absatz 1 BV sind alle wichtigen rechtsetzenden Bestimmungen, insbesondere jene, die verfassungsmässige Rechte berühren, in der Form des Bundesgesetzes zu erlassen. Dies ist mit der Vorlage gewährleistet.

5.4 Unterstellung unter die Ausgabenbremse

Artikel 159 BV sieht vor, dass Subventionsbestimmungen sowie Verpflichtungskredite und Zahlungsrahmen, die neue einmalige Ausgaben von mehr als 20 Millionen Franken oder neue wiederkehrende Ausgaben von mehr als zwei Millionen Franken nach sich ziehen, der Zustimmung der Mehrheit der Mitglieder beider Räte bedürfen. Die Vorlage enthält eine bereits bestehende Subventionsbestimmung, welche im bisherigen Rahmen (8,4 Mio.) weitergeführt werden soll. Da diese bei ihrer Schaffung nicht der Ausgabenbremse unterstellt wurde, wird dies im Rahmen der Verabschiedung des vorliegenden Gesetzes nachgeholt. Artikel 81 Absatz 5 untersteht damit der Ausgabenbremse.

5.5 Einhaltung der Grundsätze der Subventionsgesetzgebung

Die Kantone fordern in der Vernehmlassung einhellig eine Abgeltung für den im Auftrag des Bundes verursachten Aufwand und damit eine Abweichung vom Grundsatz, dass die Kantone die Vollzugskosten für Bundesrecht selber tragen. Der Gesetzesentwurf sieht in Artikel 81 Absatz 5 deshalb vor, dass der Bund die Kantone im Rahmen der bewilligten Kredite für die Leistungen, die sie zum Vollzug dieses Gesetzes erbringen, entschädigt. Der Bundesrat legt die Entschädigung aufgrund der Zahl der überwiegend für Bundesaufgaben tätigen Personen pauschal fest. Diese Regelung, die die Aufwände der Kantone nur teilweise deckt, ist identisch mit dem heute geltenden Recht (vgl. Art. 28 Abs. 1 BWIS); es soll fortgeschrieben werden und rechtfertigt sich (wie bis anhin) durch die besondere Vollzugssituation:

«… Für die Mitwirkung an der Informationsbearbeitung könnte eine Nichtübernahme der Kosten fatale Auswirkungen haben: Der Auftrag, eine

Aufenthaltsnachforschung vorzunehmen oder eine Person zu observieren, kann mit ganz unterschiedlichem Aufwand betrieben werden. Trägt der Bund die Kosten nicht mit, wäre mit vielen Negativmeldungen zu rechnen, weil einige Kantone auf das Bereitstellen des besonders ausgebildeten Personals und dessen bedrohungsgerechten Einsatz verzichten würden. […] Es ist deshalb im Interesse des Bundes, dass in den Kantonen fähige Spezialisten vorhanden sind, die aufgrund guter Kenntnisse der örtlichen Verhältnisse mit einem verhältnismässigen Aufwand die erwünschten Ergebnisse bringen können. Die Alternative, dass der Bund eigenes Personal einsetzt, wäre mit Sicherheit kostspieliger und ist aus föderalistischen Gründen unerwünscht. Eine sinnvolle Abgeltung richtet sich deshalb nach der Anzahl Personen, die in einem bestimmten Kanton überwiegend für den Bund tätig sind.»[76]

Diese Überlegungen gelten weiterhin, zumal mit dem Inkrafttreten der Vorlage die kantonalen Vollzugskosten voraussichtlich nicht abnehmen werden. Die gegenwärtigen Abgeltungen betragen insgesamt 8,4 Millionen Franken und sollen nach Inkrafttreten der Vorlage in diesem Rahmen weitergeführt werden.

5.6 Delegation von Rechtsetzungsbefugnissen

Das Gesetz enthält insofern Delegationsnormen zum Erlass von Verordnungsrecht, als der Bundesrat als Verordnungsinstanz innerhalb des vom Gesetz vorgegebenen Rahmens Verordnungsrecht erlassen darf. Diese Delegation ist erforderlich, weil sie Regelungen betrifft, deren Konkretisierungsgrad die Gesetzesebene überschreiten würde. Aufgrund der vorgegebenen Leitlinien in den Gesetzesartikeln ist die Rechtsetzungsermächtigung des Gesetzes hinreichend konkretisiert.

Im Einzelnen kann der Bundesrat zusätzlich zu seinen bestehenden Kompetenzen neu in folgenden Bereichen Bestimmungen erlassen:

- Kategorien von Waffen tragenden Mitarbeiterinnen und Mitarbeiter des NDB sowie deren Ausbildung (Art. 8 Abs. 3)
- Zusammenarbeit und Informationsaustausch zwischen dem NDB und den zuständigen Stellen des Nachrichtendienstes der Armee; Aufgabenteilung zwischen dem NDB und der Dienststelle für militärische Sicherheit während eines Friedensförderungs-, Assistenz- oder Aktivdienstes (Art. 11 Abs. 3)
- Vorgänge und Feststellungen, die dem NDB von bestimmten Behörden unaufgefordert zu melden sind; Umfang der Meldepflicht und Verfahren der Auskunftserteilung (Art. 20 Abs. 4)
- Aufklärungsbereiche, Organisation und Verfahren der Funkaufklärung sowie die maximale Aufbewahrungsdauer beim durchführenden Dienst (Art. 37 Abs. 3)
- Aufklärungsbereiche, Organisation und Verfahren der Kabelaufklärung sowie die maximale Aufbewahrungsdauer beim durchführenden Dienst (Art. 38 Abs. 4)

76 Erläuterung zu Art. 26 in der Botschaft zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit und zur Volksinitiative «S.o.S. Schweiz ohne Schnüffelpolizei», BBl **1994** II 1127, hier 1192

- Entschädigung der Betreiberinnen von leitungsgebundenen Netzen und der Anbieterinnen von Telekommunikationsdienstleistungen (Art. 42 Abs. 4)
- Weitergabe von Lagebeurteilungen und vom NDB erhaltenen Daten durch die kantonalen Vollzugsbehörden (Art. 45 Abs. 3)
- Einzelheiten der Datenbearbeitung in den einzelnen Informationssystemen (Art. 46 Abs. 2)
- Kategorien der im Informationssystem Quattro P zu erfassenden Personen (Art. 54 Abs. 4)
- Zugangsrechte, Aufbewahrungsdauer und Datensicherheit betreffend Daten aus genehmigungspflichtigen Beschaffungsmassnahmen (Art. 57 Abs. 4)
- Politische Steuerung: Erteilung des Grundauftrags; Genehmigung der Beobachtungsliste; Bestimmung der als gewalttätig einzustufenden Gruppierungen; Beurteilung der Bedrohungslage; usw. (Art. 69)
- Beauftragung des NDB in besonderen Lagen zur Wahrung wesentlicher Landesinteressen nach Artikel 3; Dauer, Zweck, Art und Umfang der erforderlichen Massnahmen (Art. 70)
- Erstellung der Beobachtungsliste (Art. 71 Abs. 3)
- Zusammensetzung und Organisation der unabhängigen Kontrollinstanz für die Funkaufklärung (Art. 75 Abs. 4)
- Finanzaufsicht über die Tätigkeitsbereiche des NDB, die besonderer Geheimhaltung bedürfen; Mindestanforderungen an die Kontrolle in den Kantonen und die Zuständigkeiten von Aufsichtsorganen des Bundes und der Kantone (Art. 76 Abs. 3)
- Kantonale Aufsicht: Beizug von unterstützenden Aufsichtsorganen für die kantonale Dienstaufsicht; Zugang zu Informationen über Bestand und Inhalt der für den Bund ausgeführten Aufträge und über die Art, wie die kantonale Vollzugsbehörde diese erledigt; Trennung der von den kantonalen Vollzugsbehörden in selbstständigem Vollzug bearbeiteten Daten von den Daten, die diese im Auftrag des NDB oder gemäss der Beobachtungsliste bearbeiten (Art. 78 Abs. 3)
- Entschädigung der Kantone für Leistungen, die zum Vollzug dieses Gesetzes erbracht werden (Art. 81 Abs. 5)

5.7 Datenschutz

Das Gesetz muss dem NDB einerseits ermöglichen, zum rechtzeitigen Erkennen und umfassenden Beurteilen von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz eine breit angelegte Informationsbasis aus vielfältigen Quellen anzulegen. Andererseits müssen die Grundrechte der von der Datensammlung betroffenen Personen so weit wie möglich gewahrt werden. Dieses Spannungsverhältnis zwischen Sicherheit und Freiheit führt zu einer differenzierten Regelung der Datenhaltung und -erfassung. Die Daten des NDB werden je nach Thematik, Quelle und Sensibilität in verschiedenen Informationssystemen abgelegt, die wiederum unterschiedlichen Regelungen unterstehen. Die strengsten Datenbearbeitungsauflagen sind für das Informationssystem mit den Daten zum

Gewaltextremismus (IASA-GEX) vorgesehen. Damit wird der Erfahrung Rechnung getragen, dass sich stets die Datenbearbeitung im Bereich des gewalttätigen Extremismus als politisch und datenschutzrechtlich besonders sensibel erwiesen hat. Die Datenbearbeitung in anderen Bereichen wie in der Spionageabwehr, in der Nonproliferation oder beim Schutz kritischer Infrastrukturen gab hingegen kaum jemals zu Kritik Anlass.

Das Gesetz regelt für jedes Informationssystem den Zweck, den Inhalt und den Benutzerkreis. Soweit ein externer Online-Zugriff vorgesehen ist, wird dies besonders ausgewiesen.

Die Vorgaben zur Datenbewirtschaftung und zur Qualitätssicherung der Daten werden im Vergleich zum aktuellen Recht nochmals verschärft. Neu wird eine lückenlose Eingangskontrolle und Triage gefordert. Voraussetzung für jede Informationsspeicherung ist immer ein genügender inhaltlicher Bezug zu den Aufgaben des NDB. Dabei muss auch sichergestellt werden, dass die Daten auf Erheblichkeit und Richtigkeit überprüft werden. Eine analoge Prüfung muss zudem erfolgen, wenn der NDB Personendaten an Dritte weitergeben möchte (z.B. in einem Analysebericht, einer Meldung an eine Behörde oder in einer Lagebeurteilung). Der NDB muss neu alle in seinen Informationssystemen gespeicherten Daten regelmässig daraufhin überprüfen, ob sie für die Erfüllung der gesetzlichen Aufgaben noch benötigt werden. Nicht mehr benötigte Daten oder Daten, die die maximale Aufbewahrungsfrist erreicht haben, werden gelöscht.

Das Gesetz sieht neu eine weitgehende Zentralisierung der Datenschutzvorgaben auf Bundesebene vor. Der Bund stellt den kantonalen Vollzugsbehörden die notwendigen Informationssysteme zur Verfügung. Er verwaltet die Daten, die nun vollständig den Regelungen des Bundes unterstehen.

Das Gesetz bestätigt das im BWIS verankerte grundsätzliche Verbot, in der Schweiz Informationen über die politische Betätigung und die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit zu sammeln.

Abschliessend ist zu erwähnen, dass ohne abweichende gesetzliche Sonderregelung die Grundsätze und Vorgaben des DSG auch für den Nachrichtendienst gelten.