

**Nachrichtendienstgesetz (NDG)**  
**Bericht zum Vorentwurf**

08. März 2013

---

## Übersicht

*Diese Vorlage soll eine einheitliche, formellgesetzliche Grundlage für den zivilen Nachrichtendienst der Schweiz (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 wie die Armee, die Aussenpolitik 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 substantiellen Beitrag für die Sicherheit der Schweiz und ihrer Bevölkerung zu leisten.*

### **Zur Vorgeschichte**

*Praktisch zeitgleich mit der Verabschiedung des Bundesgesetzes vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) hatte der Bundesrat in einem ersten Schritt die Überführung der nachrichtendienstlichen Teile des Dienstes für Analyse und Prävention (DAP) ins VBS auf den 1. Januar 2009 beschlossen. 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 eine gesetzliche Grundlage für die Aufgaben, Rechte und Pflichten und über 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.*

### **Der vorliegende Gesetzesentwurf enthält im Wesentlichen folgende Neuerungen:**

- Gesamtheitliche Gesetzesgrundlage für den NDB: Die bisherige Zerteilung in das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (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 Überwachung des Post- und Fernmelde-

verkehrs, Einsatz von technischen Überwachungsgeräten im privaten Bereich usw., werden in überarbeiteter Form neu 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 zunehmend aggressiveren Akteure, die die innere und die äussere Sicherheit der Schweiz bedrohen und angesichts der komplexeren Bedrohungsformen weiterhin wahrzunehmen. Eine gerichtliche (Bundesverwaltungsgericht) und eine politische Instanz (Chefin/Chef des VBS) sollen im Einzelfall über die Genehmigung der neuen Massnahmen entscheiden.

- Differenzierte Datenhaltung und -erfassung: 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 Partnerdienst, Lagebeurteilung) verwendet werden, müssen sie auf Richtigkeit und Erheblichkeit geprüft werden. Daten, die der NDB mittels einer bewilligungspflichtigen Beschaffungsmassnahme erhält, werden gesondert behandelt und stehen nur den 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 Parlamentes. Die Funkaufklärung unterliegt zusätzlich einer gesonderten fachlichen Überprüfung durch die Unabhängige Kontrollinstanz. Die neu beantragten, bewilligungspflichtigen Beschaffungsmassnahmen sowie die Kabelaufklärung gelangen ihrerseits nur zur Anwendung, wenn das Bundesverwaltungsgericht und anschliessend die Chefin oder der Chef des VBS dem Einsatz der betreffenden Massnahme zugestimmt bzw. diesen freigegeben haben. Mit diesen Mechanismen soll die Recht- und Verhältnismässigkeit der Tätigkeiten des NDB sicher gestellt werden.

## Inhaltsverzeichnis

<b>Übersicht</b>	<b>2</b>
<b>1 Allgemeiner Teil</b>	<b>5</b>
1.1 Einleitung	5
1.2 Vorgeschichte und Auftrag des Bundesrates	5
1.3 Entstehung des vorliegenden Gesetzesentwurfs	7
1.4 Ziele für das neue Nachrichtendienstgesetz	8
1.5 Kernpunkte des Gesetzesentwurfs	11
1.6 Rechtsvergleich und internationales Recht	13
1.7 Finanzielle, personelle und volkswirtschaftliche Auswirkungen des Gesetzesentwurfs	13
1.8 Auswirkungen des Gesetzesentwurfs auf die Zusammenarbeit mit den Kantonen	14
1.9 Rechtliche Aspekte	15
<b>2 Erläuterungen zum Gesetzesentwurf</b>	<b>17</b>

# Bericht zum Gesetzesentwurf

## 1 Allgemeiner Teil

### 1.1 Einleitung

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, Entscheidungsträger aller Stufen mit Informationen zu versorgen, die diese benötigen, um ihre Führungsaufgabe situations- und zeitgerecht wahrnehmen zu können.

Der NDB gehört wie die Aussenpolitik, die Armee, der Bevölkerungsschutz, die Wirtschaftspolitik, die Zollverwaltung, die Polizei und der Zivilschutz zu den sicherheitspolitischen Instrumenten der Schweiz. Er ist Teil der Sicherheitsarchitektur der Schweiz.

Der Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz vom 23.6.2010<sup>1</sup> (nachfolgend: sicherheitspolitischer 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 Entscheidungsträger jeglicher Ebenen geschaffen werden kann.“*

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, Tätigkeit, Beauftragung und Kontrolle des Nachrichtendienstes gesetzlich zu regeln. Damit soll der NDB in die Lage versetzt werden, im Sinne der Prävention einen substantiellen Beitrag für die Sicherheit der Schweiz und ihrer Bevölkerung zu leisten.

### 1.2 Vorgeschichte und Auftrag des Bundesrates

Im Bericht vom 29. Februar 2008<sup>2</sup> 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 SND und der DAP) überschneidet sich in einzelnen Bereichen sowohl der Natur der Sache nach als auch von der gesetzlichen Aufgabenumschreibung her. Einerseits lassen sich die*

<sup>1</sup> BBl 2010 5133

<sup>2</sup> BBl 2008 4015

äussere und die 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 Auslandskontakte 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 und VBS. 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 auf Grund 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 auf Grund der Parlamentarischen Initiative entstandene Bundesgesetz vom 3. Oktober 2008<sup>3</sup> über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) wurde am 3. Oktober 2008 von den Eidg. Räten verabschiedet und 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.

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

<sup>3</sup> SR 121

*„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 sowie die geltenden Bestimmungen sollen in der Gesetzesvorlage neu geregelt werden.“*

*Staffelung der Gesetzgebungsarbeiten gemäss BRB vom 27. November 2009*

National- und Ständerat hatten im Frühjahr 2009 die Vorlage BWIS II vom 15. Juni 2007 (Besondere Mittel der Informationsbeschaffung; „BWIS II“) zur Überarbeitung an den Bundesrat zurückgewiesen. Zu einer inhaltlichen Auseinandersetzung mit den einzelnen Gesetzesartikeln war es dabei nicht gekommen; die parlamentarische Debatte beschränkte sich auf die Eintretensfrage. Genaue Anhaltspunkte über die damalige politische Akzeptanz einzelner Elemente der Vorlage lassen sich deshalb nicht ableiten.

Der Bundesrat hatte in der Folge eine Staffelung der Gesetzgebungsarbeiten beschlossen (Bundesratsbeschluss vom 27. November 2009): In einer ersten Vorlage sollten die mehrheitlich unbestrittenen und entscheidungsreifen Anliegen realisiert werden. Dieser Teil des Konzepts wurde inzwischen durch die Zusatzbotschaft „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 bereits erwähnte Nachrichtendienstgesetz zum Gegenstand haben.

### **1.3 Entstehung des vorliegenden Gesetzesentwurfs**

Zur Vorbereitung des neuen Gesetzes hatte der NDB eine interdepartementale Arbeitsgruppe (IDAG) eingesetzt. Diese setzte sich zusammen aus Vertretern des VBS, des EDA, des BJ, von fedpol, des EDÖB, der Bundesanwaltschaft, der Kantone und des NDB.

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 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 BWIS und aus dem ZNDG sowie Neuregelungen aus der Revision BWIS II–reduziert<sup>4</sup> wurden in den Gesetzesentwurf übernommen, soweit dies als sinnvoll erschien. So entsprechen beispielsweise die besonderen Auskunftspflicht und Meldepflichten und das Tätigkeitsverbot dem Grundsatz nach den entsprechenden Bestimmungen aus der Botschaft BWIS II–reduziert.

<sup>4</sup> Zusatzbotschaft vom 27. Oktober 2010 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit („BWIS II reduziert“; BBl 2010 7841)

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.

#### *Umstrittene Punkte*

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 hatte der Bundesrat in seiner Zusatzbotschaft zur Änderung des BWIS vom 27. Oktober 2010 (BWIS II-reduziert) im Wesentlichen auf folgende genehmigungspflichtige Mittel der Informationsbeschaffung verzichtet:

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

Diese Punkte wurden im vorliegenden Entwurf für ein Nachrichtendienstgesetz wieder aufgenommen.

## **1.4 Ziele für das neue Nachrichtendienstgesetz**

### *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 substantiellen Beitrag zur Wahrung der Schweizer Interessen und der inneren wie äusseren Sicherheit der Schweiz zu liefern und zwar unter Wahrung der Freiheitsrechte 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 Einführung von bewilligungspflichtigen Beschaffungsmassnahmen. Er regelt auch die Nachrichtenbeschaffung der Kantone, bzw. der kantonalen Vollzugsbehörden im Rahmen dieses Entwurfs.

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

### *Ein 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. Das gilt für die Schweiz in besonderem Mass. Sie ist als unabhängiger und neutraler Staat in verschiedener Hinsicht auf sich alleine gestellt. Unsere Partner in Europa gehören mehrheitlich der NATO und/oder der EU an. Die Bildung von neuen Gremien wie die G20, in denen weitreichende Entscheidungen gefällt werden, die auch die Schweiz betreffen, zu denen unser Land aber kaum konsultiert wird, ergänzt dieses Bild. Gerade die Mitglieder von EU und NATO sind auch informationsmässig eng miteinander vernetzt. Die Mitgliedschaft zahlt sich in einem breiten, permanent unterhaltenen Lagebild aus. Der NDB unterstützt durch seine Kontakte zu den Nachrichtendiensten von Partnerstaaten und durch die so erhaltenen Informationen die Aussenpolitik der Schweiz.

### *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 Inland/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 eingesetzten Quellen, Mitarbeitern und 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 sogenannte Fichenaffäre 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 Verfol-

gung 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<sup>5</sup> über den Datenschutz (DSG) gerecht. Kurz nach der Inkraftsetzung 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 Eidgenössische Justiz- und Polizeidepartement (EJPD), ihm über Massnahmen zur Verbesserung 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“ 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 zur Überarbeitung an den Bundesrat zurückgewiesen. Die hauptsächlichsten Lücken und Schwächen des BWIS sind deshalb bis heute unverändert geblieben.

So ist im geltenden Recht der Post- und Fernmeldeverkehr generell jeder Gefährdungsabklärung nach 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 bezüglich verbotenen Nachrichtendienst gesammelt werden, so sind nach geltendem Recht nicht allgemein zugängliche Orte (z.B. Hotelzimmer) generell jeder Bedrohungsbekämpfung entzogen. 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 bei Terroris-

<sup>5</sup> SR 235.1

mus und 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:

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

## 1.5 Kernpunkte des Gesetzesentwurfs

### *Neuausrichtung der Informationsbeschaffung*

Der Gesetzesentwurf 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 endgültig von der sogenannten „Fichenaffäre“ Abschied genommen werden, indem eine Trennlinie zwischen eigentlichem 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 gemäss Artikel 61 Absatz 1 Buchstabe c auf einer Liste jährlich fest, welche Gruppierungen als gewaltextremistisch einzustufen sind.

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

Die in der ursprünglichen Vorlage BWIS II<sup>6</sup> enthaltenen, vom Parlament zur Überprüfung zurückgewiesenen besonderen Mittel der Informationsbeschaffung wurden hinsichtlich ihrer Verfassungs- und Völkerrechtskonformität begutachtet (Gutachten

<sup>6</sup> Botschaft vom 15. Juni 2007 zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; BBl 2007 5037)

Prof. Giovanni Biaggini vom Juni 2009<sup>7</sup>). In der vorliegenden Vorlage 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,
- Auskünfte über die Fernmelde- und Postverbindungen überwachter Personen,
- 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 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 des VBS, bzw. den Chef des VBS.

Diese neuen Beschaffungsmassnahmen werden vorgeschlagen, weil das heutige Instrumentarium (Art. 14 BWIS) nicht mehr ausreicht, um die präventive Aufgabe des Nachrichtendienstes im Bereich der inneren Sicherheit in Anbetracht der zunehmend aggressiveren und komplexeren Bedrohungsformen wahrzunehmen. Im Übrigen wird auf die Erläuterungen zu Artikel 22ff. (genehmigungspflichtige Beschaffungsmassnahmen) verwiesen.

#### *Nachvollzug der technischen Entwicklung bei den genehmigungsfreien Beschaffungsmassnahmen*

Die genehmigungsfreien Beschaffungsmassnahmen (Art. 11ff.) werden ebenfalls erweitert. Vorhandene technische Möglichkeiten (z.B. Einsatz von Drohnen) sollen nutzbar gemacht werden. Solche Mittel konnten bisher mangels formellgesetzlicher Grundlagen im Inland nicht eingesetzt werden.

#### *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 Partnerdienst, Lagebeurteilung) verwendet werden, müssen sie auf Richtigkeit und Erheblichkeit bewertet werden. Daten, die der NDB mittels einer

<sup>7</sup> VPB 4/2009 (S. 238-330)

bewilligungspflichtigen Beschaffungsmassnahme oder aufgrund von Grenzkontrollen erhält, werden gesondert behandelt und stehen nur den Spezialisten innerhalb des NDB zur Verfügung.

## **1.6 Rechtsvergleich und internationales Recht**

In der tabellarischen Zusammenstellung im *Anhang II* werden verschiedene Nachrichtendienstsysteme aus dem europäischen Umfeld der Schweiz einander in ausgewählten Punkten vergleichend gegenüber gestellt. 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.

## **1.7 Finanzielle, personelle und volkswirtschaftliche Auswirkungen des Gesetzesentwurfs**

### *Finanzielle Auswirkungen*

Die finanziellen Auswirkungen sind stark abhängig von der Art der Realisierung der einzelnen Massnahmen und der Häufigkeit von deren Anwendung. Der Bundesrat rechnet damit, dass bei der heutigen Bedrohungslage solche Massnahmen in rund 10 Fällen pro Jahr zur Anwendung kommen, wobei pro Fall mehrere Massnahmen möglich sind.

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 ca 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 der zuständige Dienst „Überwachung des Post- und Fernmeldeverkehrs“ abstützen. Hier wird bei der geschätzten Fallzahl mit einem jährlichen Gebührenanfall von ca. 500'000 Franken gerechnet.

Für Übersetzungsarbeiten der aufgezeichneten Kommunikation sind jährlich ca. 800'000 Franken zu veranschlagen.

Die Kosten für die Entschädigung der Anbieterinnen bei der Kabelaufklärung (Art. 34ff.) werden in Analogie zur Entschädigung der Fernmeldeüberwachung über den

Dienst „Überwachung des Post- und Fernmeldeverkehrs“ auf ebenfalls rund 500'000 Franken 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.

### *Personelle Auswirkungen*

Betreffend die Umsetzung der neu vorgeschlagenen Beschaffungsmassnahmen soll wo immer möglich auf den bestehenden Strukturen (NDB, Führungsunterstützungsbasis der Armee FUB, Dienst für Überwachung des Post- und Fernmeldeverkehrs im EJPD) aufgebaut werden. Insgesamt ist aber mit rund 16 zusätzlichen Stellen zu rechnen. Diese verteilen sich auf folgende neue Funktionen: Im NDB operative Techniker für die technische Betreuung der genehmigungspflichtigen Beschaffungsmittel, Analytiker für die operative Auswertung von Informationen, die mit genehmigungspflichtigen Massnahmen beschafft wurden, Juristen für das Vorbereiten der Anträge, Vollzugskontrolle und Berichterstattung im Zusammenhang mit genehmigungspflichtigen Beschaffungsmethoden, sowie weiteren Stellen für die Qualitätssicherung der neuen Systeme und die Ansteuerung der Kabelaufklärung. Weitere Stellen werden benötigt für das Bundesverwaltungsgericht für das Genehmigungsverfahren für Beschaffungsmassnahmen, das Bundesarchiv für die dezentrale Archivierung in den Räumen des NDB und das Zentrum Elektronische Operationen ZEO der FUB für den Testbetrieb der Kabelaufklärung.

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

### *Sonstige Auswirkungen*

Die Unterstützungsleistungen zu Gunsten 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.

## **1.8 Auswirkungen des Gesetzesentwurfs auf die Zusammenarbeit mit den Kantonen**

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 Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS) und mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) zusammen.



22ff. des Entwurfs enthaltene Schutz der Grundrechte bezieht sich deshalb ausschliesslich auf Personen in der Schweiz.

Die im Entwurf enthaltenen bewilligungspflichtigen Beschaffungsmassnahmen tragen dem Erfordernis nach einer formellgesetzlichen Grundlage Rechnung, die auch dem Bestimmtheitsgebot genügt. Das vorgeschlagene Konzept berücksichtigt ferner das Prinzip der Verhältnismässigkeit und das Vorliegen 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 körperliche Untersuchungen oder die Anwendung körperlichen Zwangs). Solche Massnahmen sind Polizeibehörden vorbehalten, die zur Erfüllung ihrer Aufgaben polizeilichen Zwang oder polizeiliche Massnahmen einsetzen dürfen (vgl. Zwangsanwendungsgesetz<sup>9</sup>).

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 3 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 ausländischer Staatsbürger (z.B. die Wahrung der Privatsphäre) tangiert werden können.

Die Informationsbeschaffung im Ausland soll deshalb nur erfolgen, wenn die zur Gefahrenabwehr benötigten Informationen im Inland nicht beschafft werden können. Sie dient zur Abwehr von Gefahren für die Schweiz, die ihr aus sicherheitspolitisch bedeutsamen Vorgängen im Ausland, z.B. in den Bereichen Terrorismus, Proliferation und Entwicklung von machtpolitischen Verhältnissen, entstehen können.

Im Spannungsfeld zwischen den Sicherheitsinteressen der Schweiz und dem Schutz der Grundrechte ausländischer Staatsangehöriger, bzw. von Personen im Ausland, überwiegt nach dem Konzept dieser Vorlage grundsätzlich das Sicherheitsinteresse. Der Grundrechtsschutz von Personen im Ausland soll gegenüber demjenigen von Personen im Inland weniger umfassend berücksichtigt werden.

In jedem Fall zu berücksichtigen ist jedoch der Grundsatz der Verhältnismässigkeit: Der Eingriff in Grundrechte und der erwartete Informationsgewinn dürfen in keinem Missverhältnis zueinander stehen.

Der gegenüber dem Inland weniger weit gehende Grundrechtsschutz betrifft vor allem die Beschaffungsmassnahmen im Sinne von Artikel 22 des Entwurfs. Gegen eine zum Inland analoge Bewilligungspflicht sprechen - abgesehen von den oben erwähnten grundsätzlichen Überlegungen - folgende Gründe:

- Für eine schweizerische Bewilligungsinstanz wäre es auf Grund 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.

<sup>9</sup> SR 364

- Die Bewilligung 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 bewilligungspflichtigen Beschaffungsmassnahmen. Davon ausgenommen ist das Eindringen in Computersysteme und -netzwerke, die sich im Ausland befinden (Art. 32 Abs. 2).

### *Abgrenzung von der Tätigkeit der Strafverfolgungsbehörden*

Im Gegensatz zu den Strafverfolgungsbehörden, deren Tätigkeit letztlich auf die Überführung des Täters gerichtet ist (repressive Zielsetzung), hat der NDB eine präventive Aufgabe. Der Gesetzesentwurf betont im Zweckartikel den präventiven Charakter der getroffenen Massnahmen (Informationsbeschaffung, Beurteilung der Bedrohungslage). Ziele sind das frühzeitige Erkennen von Bedrohungen der inneren oder äusseren Sicherheit der Schweiz und die Sicherung ihrer demokratischen und rechtsstaatlichen Grundlagen.

Wenn der NDB im Rahmen seiner Abklärungen auf strafbare Handlungen oder auf den Verdacht von strafbaren Handlungen stösst, informiert er die Strafverfolgungsbehörden.

## **2 Erläuterungen zum Gesetzesentwurf**

### *Vorbemerkungen:*

#### *Zum Begriff Bedrohung:*

Der Begriff „Bedrohung“ setzt nach der Definition des Bundesrates im sicherheitspolitischen Bericht „*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)<sup>10</sup>.

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 auch den Charakter einer Chance haben können, die eine Bedrohungen verhindert oder abwendet.

#### *Selbsterklärende Artikel:*

Artikel und Absätze, die selbsterklärend sind und keine zentrale Rolle im Gesetzestext spielen, werden in den Erläuterungen zur Vernehmlassungsvorlage nicht behandelt, um den Text schlank zu halten. Falls die Vernehmlassungsergebnisse Missverständnisse dokumentieren sollten, kann später eine Kommentierung in der Botschaft erfolgen.

<sup>10</sup> BB1 2010 5146

*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 und äusseren Sicherheit. Nach neuerer Auffassung ist diese Regelungskompetenz in Artikel 173 Absatz 2 der Bundesverfassung enthalten (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 7 (Kantonale Vollzugsbehörden) und 73 (Vollzug durch Kantone).

## **1. Kapitel: Allgemeine Bestimmungen und Grundsätze der Informationsbeschaffung**

### *Art. 1*            Gegenstand und Zweck

Die Einführung einer Zweckbestimmung erscheint im Hinblick auf die Bedeutung des vorliegenden Gesetzesentwurfs als Gesamtkodifikation für den Nachrichtendienst der Schweiz als angebracht.

Während *Absatz 1* nur den Inhalt des Gesetzestextes zusammenfasst, übernimmt *Absatz 2* Elemente des BWIS und hat einen programmatischen Charakter. Er definiert die Zwecke, an welchen sich letztlich die nachrichtendienstlichen Tätigkeiten ausrichten. *Absatz 2* ist damit nicht kompetenzbegründend, wirkt aber als Leitlinie für den Vollzug des Gesetzes.

*Absatz 3* soll es dem Bundesrat ermöglichen, den NDB in besonderen Lagen mit der Informationsbeschaffung und –auswertung sowie gegebenenfalls operativen Tätigkeiten zu beauftragen, die über den ordentlichen Auftrag des NDB hinausgehen. Hierzu ist ein besonderer Beschluss des Bundesrates nach Artikel 62 notwendig. Der NDB darf also nicht von sich aus 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. 22ff.), 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 ausschliesst (z.B. genehmigungspflichtige).

In der Regel wird es bei der Anrufung solcher, im allgemeinen gesetzlichen Auftrag des NDB noch nicht enthaltenen weiteren Landesinteressen um die Auslandsaufklärung gehen.

Dieser Absatz 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. 7a bis 7d des Regierungs- und Verwaltungsorganisationsgesetzes, SR 172.010).

### Art. 3 Grundsätze der Informationsbeschaffung

Die Hauptaufgabe des Nachrichtendienstes besteht im Beschaffen und Beurteilen von Informationen und deren Weitergabe in Form von nachrichtendienstlichen Produkten an berechnigte Empfänger oder in der Umsetzung der Erkenntnisse in präventive operative Leistungen zur Verringerung der Bedrohungen der Sicherheit. Deshalb definiert der Gesetzesentwurf in Artikel 3 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 Gegenstände 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. 11) 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 detailliert aufgestellte System der genehmigungsfreien und der genehmigungspflichtigen Massnahmen. Ihre Anwendung ist dort geregelt. Die genehmigungsfreien Beschaffungsmassnahmen (Art. 11ff.) 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. 22ff.) 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 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 DSGVO). Die Regelung entspricht den heutigen Artikeln 5 Absatz 1 ZNDG und 14 Absatz 1 BWIS. Eine Beschaffung und Bearbeitung mit Wissen der betroffenen Personen würde den Zweck der Datenbearbeitung in der Regel vereiteln. Hingegen besteht ein Auskunftsrecht, das in Artikel 58 geregelt ist.

Die *Absätze 5 bis 8* übernehmen sinngemäss bestehende und bewährte Grundsätze des Schutzes der politischen Betätigung vor nachrichtendienstlicher Beobachtung und deren Ausnahmen aus dem BWIS. Das NDG gewährleistet so vollständig den gleichen Schutz wie das BWIS für Vorgänge im Inland. 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 5 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 Anbieterpflicht an das Bundesarchiv. Nicht archivwürdige Daten werden definitiv vernichtet.

*Absatz 8* stellt klar, dass über Organisationen und Gruppierungen der Beobachtungsliste nach Artikel 63 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 das vermieden.

## **2. Kapitel: Aufgaben und Zusammenarbeit des NDB**

### **1. Abschnitt: Aufgaben, Schutz- und Sicherheitsmassnahmen sowie Bewaffnung**

#### *Einleitende Bemerkungen:*

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 (siehe Art. 60).

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 zu Händen der zuständigen Behörden Bericht zu erstatten. So sollen die Risiken minimiert werden. Der NDB nimmt aber keine polizeilichen oder strafprozessualen Aufgaben wahr (z.B. Ermittlungen, Festnahmen, usw.). Nachrichtendienst und Strafverfolgung ergänzen sich somit. Jedoch ist nicht eines die Vorstufe des anderen. 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. 4 Aufgaben des NDB

Das Gesetz erwähnt in *Absatz 1* nur den NDB als vollziehende Behörde. Die Aufgabenbereiche von Buchstabe a gelten jedoch auch für den Vollzug in den Kantonen (vgl. Art. 73). 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 verbotenen Nachrichtendienst oder Terrorismus verbunden sind, fallen sie zwar wie bisher auch unter die in Ziffer 1 und 2 definierten Aufgaben. Da dieser Hintergrund oft aber – wenn überhaupt – erst nach eingehenden Abklärungen ersichtlich ist, ist es zur Sicherung der Rolle des NDB in der Cyberstrategie des Bundes notwendig, dessen Beteiligung an der Bearbeitung von Anfang an zu ermöglichen. Die Netzwerke der kritischen Infrastrukturen müssen gegen Angriffe von Hackern geschützt werden. Der NDB soll hier zu Handen 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 „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 demokratischen und rechtsstaatlichen Ordnung zu gefährden sowie ihr schweren sicherheitspolitischen oder anderweitigen Schaden zuzufügen oder die Handlungsfähigkeit ihrer Behörden zu beeinträchtigen.

Buchstabe c bezieht sich auf die essentielle Aufgabe des NDB, der Landesregierung zeitgerecht für die Erfüllung ihrer Aufgaben notwendige Informationen zu liefern. Die Aufgabe: „Wahrung der Handlungsfähigkeit der Schweiz“ wurde deshalb ausdrücklich in den Aufgabenkatalog des NDB aufgenommen.

Ebenfalls neu aufgenommen wurde der Begriff „Wahrung weiterer wesentlicher Landesinteressen“ (vgl. Erläuterungen zu Art. 1 Abs. 3).

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. das jährliche WEF oder grosse internationale Konferenzen wie der 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 berechtigten beteiligten Stellen das ständige Verfolgen der aktuellen Lage über die Elektronische Lagedarstellung ELD (vgl. Art. 48).

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 Partnerdiensten sollen auf diese Weise vermieden werden. Weiter präzisiert ist diese Aufgabe in Artikel 10.

*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 5 hinaus und wird deshalb hier ausdrücklich geregelt.

*Absatz 7* hat schliesslich besondere Bedeutung für die Sicherheit des NDB, seiner Mitarbeitenden und seiner Informationen. Artikel 5 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 60 separat geregelt.

#### *Art. 5* 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 Mitarbeitenden des NDB aber auch bei temporär eingesetztem Personal wie beispielsweise Praktikanten oder Angehörigen der Armee. Ebenfalls kontrolliert werden können Mitarbeitende von Firmen, die in den Räumlichkeiten des NDB Dienstleistungen erbringen. Nicht Gegenstand von Kontrollen sind Mitglieder der Aufsichtsorgane und Besucher. Diese werden in den Räumen des NDB ständig begleitet.

*Buchstabe c:* Videoüberwachungssysteme 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 und/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 Schutzmass-

nahmen (Schirmdämpfung und akustische Dämmung) ausgestattet, dass ein unerlaubter Informationsabfluss z.B. via Mobiltelefone verunmöglicht wird. Dort 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 sensibler oder geheim klassifizierter Gespräche. Die entsprechenden Geräte müssen den Vorschriften des BAKOM 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.

#### *Art. 6*                      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 Mitarbeitenden 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 Mitarbeitenden 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 eines Mitarbeitenden in der Beschaffung Inland ist in den geschilderten Fällen vergleichbar mit derjenigen eines Führers von Vertrauenspersonen (VP-Führers) im polizeilichen Bereich.

Die Waffe darf nur zur Notwehr (Art. 15f. Strafgesetzbuch<sup>11</sup>) oder in Fällen von Notstand (Art. 17f. Strafgesetzbuch) eingesetzt werden. Die Verhältnismässigkeit insbesondere des Schusswaffeneinsatzes ist zu wahren (Abs. 2).

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

## **2. Abschnitt: Zusammenarbeit**

#### *Art. 7*                      Kantonale Vollzugsbehörden

Der Vollzug der nachrichtendienstlichen Aufgaben nach diesem Gesetzesentwurf erfolgt durch Bund und Kantone gemeinsam (vgl. Art. 73). Die kantonalen Vollzugsbehörden beschaffen auf ihrem Gebiet Informationen, die sie direkt auf Grund 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.

<sup>11</sup> SR 311.0

Weitere Vorschriften mit Bezug auf die Kantone befinden sich in den Kapiteln 4 (betreffend Datenbearbeitung) und 6 (betreffend Kontrolle und Aufsicht).

#### *Art. 8* 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 Konferenz der kantonalen Polizeikommandanten und die Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren. 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.

#### *Art. 9* 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 9 regelt dabei die Pflicht des NDB, die zuständigen Stellen der Armee über armeerelevante Vorgänge zu informieren. Deren Informationspflichten sind hingegen in den Artikeln 17 und 18 (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 Partnerdiensten 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. Sie sind damit keine „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.

#### *Art. 10* Zusammenarbeit mit dem Ausland

Einleitend ist darauf hinzuweisen, dass der Bundesrat 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 schon Kraft der Bestimmung von Artikel 56 Absatz 3 der Bundesverfassung. Am bisherigen Vollzug durch die Kantone 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. Dies findet heute durch den NDB mit Partnerdiensten 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. Gleiches gilt auch für die Schweiz.

Eine Ausnahme könnte sich in Zukunft vor allem bezüglich den Betrieb von gemeinsamen internationalen Informationssystemen ergeben (Buchstabe 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 dafür 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. 61 Abs. 3).

Gemäss *Absatz 2* soll es künftig möglich sein, 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.

*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<sup>12</sup> 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.

### **3. Kapitel: Informationsbeschaffung**

Nach der umfassenden Definition des Datenbearbeitungsbegriffes im DSG ist zwar die Beschaffung im Begriff der Bearbeitung enthalten (vgl. Art. 3 Bst. e DSG). Da

<sup>12</sup> SR 121.1

die Beschaffung der Daten jedoch für einen Nachrichtendienst zum einen von zentraler Bedeutung ist und zum anderen aus Sicht der betroffenen Personen mit den 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 Vollzugaufträge nach den Artikeln 7 und 73 jedoch auch für die kantonalen Vollzugsbehörden.

### **1. Abschnitt: Genehmigungsfreie Beschaffungsmassnahmen**

In diesem Abschnitt sind jene Beschaffungsmassnahmen aufgeführt, die der NDB selbständig und ohne besondere externe Bewilligung einsetzen kann, weil die Eingriffsintensität relativ gering ist. Sie entsprechen weitgehend den heute in Artikel 14 Absatz 2 BWIS geregelten Beschaffungsmöglichkeiten. Das Kapitel erwähnt alle klassischen nachrichtendienstlichen Beschaffungsmittel von der „open source intelligence“ (OSINT, Art. 12) über die „imagery intelligence“ (IMINT, Art. 12 Abs. 2), „human intelligence“ (HUMINT, Art. 13) bis zur „communication intelligence“ (COMINT, Art. 24 und 33ff). Für ihre Anwendung stellt das NDG je nach Intensität des Grundrechtseingriffes besondere Regeln auf.

#### *Art. 11*      Öffentliche Informationsquellen

Ein Nachrichtendienst schöpft viele Informationen aus dem öffentlichen Bereich. Dies erlaubt ihm, mit besonderen nachrichtendienstlichen Mitteln nur 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 öffentlich, das heisst praktisch jedermann zugängliche Informationen handelt. Die Tatsache, dass bestimmte Informationen nur gegen Bezahlung angeboten werden, ändert am öffentlichen Charakter nichts. Elektronische Datensammlungen sollen hier nicht anders behandelt werden als klassische Medien wie Zeitungen oder Fachpublikationen, die in der Regel auch gegen Entgelt angeboten werden.

Die Qualität dieser Informationen kann sehr unterschiedlich sein, weshalb ihre Beurteilung bei der Verwendung wichtig ist. Der Gesetzesentwurf sieht deshalb vor, die OSINT-Informationen innerhalb des NDB auf einem besonderen Informationssystem verfügbar zu machen (Art. 49). Von dort aus können sie bei Bedarf beurteilt und bei Verwendung für nachrichtendienstliche Produkte in weitere Systeme überführt werden.

#### *Art. 12*      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, dass es sich bei ihm um einen gewöhnlichen Diplomaten handle.

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

*Absatz 2* regelt neu den engeren Bereich der nachrichtendienstlichen Bildaufklärung (IMINT). Zur Erfüllung der gesetzlichen Aufgaben kann es in Einzelfällen notwendig sein, geeignete luftgestützte Mittel wie Drohnen, Flugzeuge oder Hubschrauber einzusetzen. Auch weltraumgestützte Mittel wie Satelliten können geeignete Bildaufklärungsmittel darstellen (z.B. bei Entführungsfällen von Schweizer Bürgern im Ausland). Auch der Fortschritt von Bauten zu ausländischen Massenvernichtungswaffenprogrammen lässt sich anhand von Satellitenbildern gut beobachten. Der NDB verfügt selbst nicht über solche Mittel, kann ihren Einsatz aber bei Dritten veranlassen. Der schweizerische Militärische Nachrichtendienst 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 lange ein Zeitraum 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 dem privaten Grundstück abspielen. Sollen solche Vorgänge gezielt beobachtet werden, muss für die Informationsbeschaffung eine bewilligungspflichtige Massnahme nach Artikel 22ff. beantragt werden. In den anderen Fällen müssen die Daten vernichtet werden, wenn der private Raum nicht schon bei der Beobachtung ausgespart werden konnte. Die Situation ist vergleichbar mit dem Überflug eines Passagierflugzeugs über bewohntem Gebiet. Es lässt sich auch dort nicht verhindern, dass Passagiere durch die Fenster Vorgänge im privaten Raum auf dem Boden beobachten oder fotografieren. Jedoch wäre die Verwertung solcher Aufnahmen rechtlich anfechtbar.

Im Militärgesetz vom 3. Februar 1995<sup>13</sup> (MG) soll eine analoge Regelung für den militärischen Bereich verankert werden (Art. 99 Abs. 1<sup>quater</sup>, vgl. Änderung bisherigen Rechts).

### *Art. 13*            Menschliche Quellen

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

<sup>13</sup> SR 510.10

Menschliche Quellen, oder auch *Human Intelligence (HUMINT)* ist ein international anerkannter nachrichtendienstlicher Ausdruck 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 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, und/oder um eine Bezahlung für Informationen, die für die Aufgabenerfüllung des NDB von grossem Nutzen sind. Insbesondere Quellen im Ausland verlangen vielfach Geld für die Weitergabe ihrer 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 Sozialversicherungen unterliegen. Ansonsten kann die Sicherheit vieler Quellen nicht gewährleistet werden, und eine Zusammenarbeit ist verunmöglichlicht. Nur in besonderen Fällen können die Einkünfte bisweilen über Tarnstrukturen offiziellisiert werden.

#### *Absätze 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 in Bereichen von terroristischen Zellen zu, gewalttätigen extremistischen Gruppierungen aus dem Ausland, aber auch in Bereichen, wo 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:

- Atomwissenschaftler 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 Regimegegnern wiederholt der Beobachtung oder Drangsalierung durch regierungstreue Personen aus ihrem Heimatland ausgesetzt war. Würde eine allfällige Zusammenarbeit von Quellen aus dem Umfeld der Regimegegner 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 bestmöglichst 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 Legendierung oder Tarnidentität durch den NDB nach Artikel 15 oder 16 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 angewogen werden können.

#### *Art. 14* Ausschreibung von Personen und Fahrzeugen zwecks Aufenthaltsfeststellung

Mit den *Absätzen 1 und 2* soll eine ähnliche Regelung eingeführt werden, wie sie das neue Polizeiaufgabengesetz vorsieht (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 weiterer wesentlicher Landesinteressen. Die Bedrohung der inneren oder äusseren Sicherheit, bzw. ein Bundesratsbeschluss betreffend die Wahrung weiterer wesentlicher Landesinteressen (vgl. Art. 1 Abs. 3 in Verbindung mit Art. 62), bildet deshalb die Voraussetzung für die Ausschreibung von Personen und Fahrzeugen durch den NDB (vgl. Abs. 2 Bst. a).

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 Terrorismus-verdächtiger Gruppierungen) feststellen zu können. Die Polizeigesetzgebung verwendet hierfür den Begriff der „verdeckten Registrierung“, der im NDG aber nicht verwendet wird, um Missverständnisse zu vermeiden. Zusätzlich soll das zukünftig auch im nationalen Teil des Schengener Informationssystems (N-SIS) erfolgen können. Wenn solche vom NDB ausgeschrie-

bene Personen den Schengen-Raum betreten bzw. verlassen oder wenn sie innerhalb des Schengen-Raums von der Polizei oder von den Grenzkontrollorganen kontrolliert werden, wird die Schweiz, bzw. der NDB, künftig von den zuständigen ausländischen Behörden eine Mitteilung erhalten. Diese erfolgt über das Schweizer SIRENE-Büro (Verbindungsstelle der für die SIS-Zusammenarbeit zuständigen Behörden der Schengen-Staaten; vgl. Art. 8 und 9 der N-SIS-Verordnung, SR 362.0). 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 von Berufsgeheimnissen und Medienschaffende).

## **2. Abschnitt: Legendierungen und Tarnidentitäten**

### *Einleitende Bemerkungen*

Der Strategische Nachrichtendienst SND verfügte seit 1997 auf der Basis von Artikel 99 des Militärgesetzes über die Möglichkeit, seine Beschaffungsorgane mit Tarnidentitäten auszustatten (vgl. Jahresbericht 2002/2003 der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation vom 23. Januar 2004; BBl 2004 1743). 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 Mitarbeitenden 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 14c 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, bei der Chefin oder dem Chef des VBS beantragt werden. Ausserdem wurde in Artikel 14c Absatz 1 Buchstabe c BWIS neu auch die Ausstattung von menschlichen Quellen des NDB mit Tarnidentitäten im Rahmen einer bestimmten Informationsbeschaffung ermöglicht.

Die Artikel 15 und 16 unterscheiden neu zwischen den Begriffen „Legendierung“ und „Tarnidentität“, da es sich um unterscheidliche Massnahmen handelt, die unabhängig voneinander eingesetzt werden können.

Die unterschiedlichen bisherigen Regelungen für die Genehmigung der Tarnidentitäten werden im vorliegenden Entwurf zusammengefasst und gelten sowohl für die Informationsbeschaffung im Ausland wie im Inland. Neu wird dem permanenten Schutzcharakter mehr Rechnung getragen. In Berücksichtigung der neu geschaffenen

nen 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 sollen 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. 15*            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 andere biographische 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 ihr 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 Mitarbeitender des NDB für eine verdeckte Beschaffungsaktion ins Ausland zu reisen und dabei als nachrichtendienstlicher Mitarbeitender identifizierbar zu sein. Ansonsten könnten die betreffenden Mitarbeitenden und die Quellen, mit denen sie in Kontakt stehen, möglicherweise enttarnt und damit gefährdet werden. Auch in der Schweiz können Mitarbeitende des NDB und ihre Quellen, insbesondere im Umfeld des Terrorismus oder des verbotenen Nachrichtendienstes, gefährdet werden, wenn ein Bezug der entsprechenden Mitarbeitenden 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 daher die Möglichkeit der Legendierung der wahren Identität notwendig.

Der Aufbau von Legendierungen 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, Mail usw.) Zeitspanne benötigt werden.

Die Verwendung von Legendierungen entspricht der bisherigen Praxis der Auslandsbeschaffung, 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 werden. Das kann z.B. der Fall sein, wenn für die Glaubhaftigkeit der Legendierung bestimmte amtliche Urkunden benötigt werden (z.B. für das Glaubhaftmachen einer bestimmten Geschäftstätigkeit).

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

## Art. 16 Tarnidentitäten

Eine Tarnidentität gibt einer Person eine andere Identität, das heisst einen anderen Namen und allenfalls andere biographische Daten (Geburtsdatum, Geburtsort usw.). Sie unterliegt deshalb wesentlich strengeren Voraussetzungen als die blosser Legenderung. Tarnidentitäten können wie die Legenderung auch die Verschleierung des Bezuges zum NDB, bzw. das Vorgeben eines anderen Arbeitgebers als der NDB enthalten. Wenn es hingegen lediglich um den Schutz des Mitarbeitenden 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 Mitarbeitenden der Informationsbeschaffung im Ausland und in bestimmten Umfeldern im Inland auf die Verwendung von Tarnidentitäten und dazugehörigen Legenderungen angewiesen. Rückschlüsse auf die wahre Identität der Mitarbeitenden der Beschaffung, z.B. im Umfeld des Terrorismus oder des verbotenen Nachrichtendienstes, können die Mitarbeitenden und auch ihre Familienangehörigen direkten Druckversuchen, Drohungen und auch konkreten physischen Bedrohungen aussetzen. Tarnidentitäten sind daher in erster Linie eine permanente Schutzmassnahme für die Mitarbeitenden, 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 eines Mitarbeitenden 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 Falles 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 Mitarbeitenden eine grundlegende Aufgabe des Dienstes, die wegen der Verwendung von falschen Identitätsdokumenten von der Chefin oder dem Chef des VBS genehmigt werden muss. Die Verwendung der Tarnidentitäten ist befristet und kann bei Bedarf verlängert werden (siehe 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 Legenderungen zur wahren Identität (Art. 15) sind die Anforderungen an Legenderungen zu Tarnidentitäten und deren Aufbau oftmals aufwändiger, da sie eine andere (fiktive) Identität mit (plausiblen) 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 dazugehörige 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 Mitarbeitenden 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 willkürlichen Höchstdauer verfallen, sondern muss sich nach den dienstlichen Bedürfnissen richten.

Um die notwendige Flexibilität zu wahren und 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.

### **3. Abschnitt: Auskunftsrechte und -pflichten**

#### *Art. 17*           Auskunftspflicht bei einer konkreten Bedrohung

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

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 Bürgern 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.

Soweit die Auskunftspflicht durch die Wahrung weiterer wesentlicher Landesinteressen begründet wird, bedarf sie eines entsprechenden Beschlusses des Bundesrates (vgl. dazu auch Erläuterungen zu Art. 1 Abs. 3 und Art. 62).

Der Artikel entspricht weitgehend dem mit BWIS II neu eingeführten Artikel 13a BWIS. Nicht mehr separat aufgeführt sind die im BWIS noch besonders erwähnten Steuerbehörden. Diese unterstehen ebenfalls der Auskunftspflicht, da sie zu den in Absatz 1 genannten Dienststellen gehören. Eine besondere Erwähnung würde zudem fälschlicherweise den Eindruck erwecken, dass Steuerbehörden dem NDB besonders oft Informationen liefern würden. Dies trifft indessen nicht zu.

Zu den auskunftspflichtigen Dienststellen 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 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997<sup>14</sup>, (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.

Die bei den Behörden und Organisationen eingeholten Auskünfte gehen an den NDB. Die Vollzugsbehörden der Kantone können im Auftrag des Bundes tätig werden und bei den auskunftspflichtigen Behörden und Organisationen Auskünfte einholen, um sie dem NDB zur Verfügung zu stellen. Datenherr ist in jedem Fall der Bund.

*Absatz 4* regelt den Fall, dass eine dritte Behörde selbständig 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 22a des Bundespersonalgesetzes vom 24. März 2000<sup>15</sup>, der Angestellte von Bundesbehörden verpflichtet, jeden Verdacht auf eine von Amtes wegen zu verfolgende strafbare Handlung zur Anzeige zu bringen.

<sup>14</sup> SR 172.010  
<sup>15</sup> SR 172.220.1

#### Art. 18 Besondere Auskunfts- und Meldepflicht

*Absatz 1* nennt die dem Vollzug von Sicherheitsaufgaben besonders nahe stehenden Behörden und Amtsstellen, die zur Erstattung von Auskünften verpflichtet sind. Die Auskunftsspflicht geht dabei weiter als diejenige nach Artikel 17 (Allgemeine Auskunftsspflicht), in dem sie nicht auf einzelne Themenbereiche beschränkt und auch nicht an besondere Voraussetzungen gebunden ist. Sie dient dem Vollzug des Gesetzes als solchem. Sie ist dafür anders als in Artikel 17 auf den genannten Kreis von Amtsstellen beschränkt.

Gemeint ist nicht eine integrale Auskunftsspflicht, sondern eine die sich auf konkrete Fälle und Organisationen bezieht.

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

*Absatz 4* entspricht dem geltenden Recht von Artikel 11 Absatz 2 Buchstabe a BWIS. Ein grösserer Teil der Meldepflichten ist im Anhang I der 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.

#### Art. 19 Verfahren bei Meinungsverschiedenheiten über Auskunfts- und Meldepflichten

*Absatz 1* regelt den Fall von Meinungsverschiedenheiten innerhalb der Bundesverwaltung. Entscheidungsinstanz 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. Das entspricht der allgemeinen Regelung der Verwaltungsorganisation.

*Absatz 2* regelt den Fall von Meinungsverschiedenheiten zwischen Bund und Kantonen. Dann ist das Bundesverwaltungsgericht zuständig. Als Gegenstück dazu wird im Bundesgesetz vom 17. Juni 2005<sup>16</sup> über das Bundesverwaltungsgericht (VGG) eine entsprechende Zuständigkeit des Bundesverwaltungsgerichts für Streitigkeiten geschaffen (siehe Änderungen bestehenden Rechts).

#### Art. 20 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 Legendierungen, welche die Zugehörigkeit zu nachrichtendienstlichen Dienststellen verschleiern, kann die befragte Person allerdings nicht auf diese Freiwilligkeit aufmerksam gemacht werden, weil sonst die Legendierung aufgedeckt werden müsste. Untersteht eine meldende oder auskunftserteilende Person einem Berufsgeheimnis oder anderen gesetzlichen Geheimhaltungsvorschriften, muss sie diese gegenüber dem NDB, bzw. den kantonalen Vollzugsbehörden beachten, wie gegen jede andere Person oder Amtsstelle auch.

*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. 21*            Besondere Auskunftspflichten Privater

*Absatz 1* übernimmt die 2012 mit Artikel 13c in das BWIS aufgenommene Verpflichtung zur Auskunftgabe für gewerbliche Transporteure und erweitert diese noch um Auskünfte von privaten Betreiberinnen und Betreibern von Sicherheitsinfrastrukturen wie Videoüberwachungsanlagen. Auch elektronische Zutrittssysteme könnten vergleichbare, wichtige Informationen liefern. Wie schon unter dem BWIS ist niemand dadurch verpflichtet, bestimmte Daten zu erheben oder aufzubewahren. Die Bestimmung soll lediglich in Fällen von konkreten Bedrohungen Zugang zu ohnehin vorhandenen Daten gewährleisten.

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.

*Absatz 2* verweist auf die schon heute gemäss Fernmeldegesetz vom 30. April 1997<sup>17</sup> (FMG) bestehende Möglichkeit, über den Dienst „Überwachung Post- und Fernmeldeverkehr“ im EJPD Informationen über Fernmeldeanschlüsse einer Person und andere ihr zugeteilte Adressierungselemente einzuholen, bzw. darüber welcher Person bekannt gewordene Adressierungselemente (z.B. Telefonnummern) zugewiesen sind. Entsprechend wird auch Art. 14 Abs. 2<sup>bis</sup> FMG angepasst.

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 des Strafgesetzbuches (Ungehorsam gegen eine amtliche Verfügung).

Verfügungen des NDB können nach Artikel 71 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 Transportunternehmens als nutzlos erweisen. Deshalb sieht die Vorlage vor, dass eine Beschwerde keine aufschiebende Wirkung hat (Art. 71 Abs. 3).

### **4. Abschnitt: Genehmigungspflichtige Beschaffungsmassnahmen**

#### *Einleitende Bemerkungen*

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.

<sup>17</sup> SR 784.10

Die nachrichtendienstlichen Organe von Bund und Kantonen sehen sich vor allem im Bereich des Terrorismus mit zunehmend 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 Kaida 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 betreffend die Radikalisierung wie im Fall von Toulouse und Montauban 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 nur sehr schwer Erkenntnisse über Tätigkeiten und Absichten 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 bedingt erfüllen. Viele Vorgänge zur Beurteilung von Bedrohungen finden nicht im öffentlichen Raum statt. Konspirative Kommunikation kann kaum im allgemeinen Internet 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 sowie Durchsuchen eines Hotelzimmers der gleichen Person). Es geht dabei um Fälle mit besonderem Bedrohungspotential in den Bereichen Terrorismus, verbotener Nachrichtendienst, Proliferation und Angriffe auf kritische Infrastrukturen oder Wahrung weiterer wesentlicher Landesinteressen, in denen die anderen Beschaffungsmassnahmen nicht ausreichen, um für die Wahrung der Sicherheit der Schweiz elementare Informationen zu erhalten.

Die genehmigungspflichtigen Beschaffungsmassnahmen umfassen insbesondere (Art. 22):

- die Überwachung des Post- und Fernmeldeverkehrs einer Person oder eines Anschlusses;
- das Orten des Standortes von Personen oder Sachen durch die Lokalisierung eines von der Person verwendeten Mobiltelefongerätes 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; und
- 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 der Direktor des NDB den sofortigen Einsatz einer Massnahme anordnen. Der Antrag an das Bundesverwaltungsgericht muss sodann innert 24 Stunden erfolgen (Art. 27 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. 55). 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. genügen die Verdachtslagen teilweise noch nicht, um strafrechtliche Ermittlungen auszulösen.

#### *Art. 22* Arten von genehmigungspflichtigen Beschaffungsmassnahmen

*Absatz 1 Buchstabe a* ermöglicht es dem NDB, die Überwachung des Post- und Fernmeldeverkehrs anzuordnen. Im Gegensatz zu den Strafverfolgungsbehörden, die solche Überwachungen im Rahmen eines Strafverfahrens zur Überführung des 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 auf strafbare Handlungen oder auf den Verdacht von strafbaren Handlungen stösst, wird er die Strafverfolgungsbehörden informieren.

*Buchstabe b* betrifft, im Unterschied zur Massnahme nach Buchstabe a, einen Anschluss der von verschiedenen Personen benutzt wird oder dessen Inhaber nicht identifiziert ist. Es kann sich z.B. um eine öffentliche Telefonkabine oder um eine anonyme Prepaid-Karte handeln. Die Überwachung dient in solchen Fällen oft auch der Identifizierung der Person, die den Anschluss benutzt und von der die Bedrohung ausgeht.

In technischer Hinsicht übernimmt der NDB das Verfahren gemäss Bundesgesetz vom 6. Oktober 2000<sup>18</sup> betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), wie es im Rahmen der Strafverfahren von Bund und Kantonen angewendet wird. Die Überwachung selbst wird vom Dienst „Überwachung Post- und Fernmeldeverkehr ÜPF“ vollzogen. Der NDB führt in diesem Bereich keine selbstständigen Überwachungen durch.

Der NDB entschädigt den Dienst ÜPF für Überwachungen nach Buchstaben a-d nach den normalen Ansätzen. Artikel 16 BÜPF regelt die Entschädigungen und wird auch auf den NDB direkt anwendbar 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<sup>19</sup>).

*Buchstabe c* ermöglicht die sogenannte rückwirkende Überwachung von Verbindungen von Post- oder Fernmeldeanschlüssen durch die die Erhebung sogenannter Randdaten oder Verbindungsnachweise. Diese Erhebung wird über den Dienst ÜPF beim Provider durchgeführt und ermöglicht es festzustellen, zu welcher Zeit ein bestimmter Fernmeldeanschluss mit welchen anderen Fernmeldeanschlüssen in Verbindung stand. Nicht möglich sind hier Auskünfte über den Inhalt der Kommunikationen.

Beispiel: Ein sich in der Schweiz unter operativer Tarnung aufhaltender ausländischer Nachrichtendienstoffizier versucht, menschliche Quellen zu rekrutieren und von diesen illegal Informationen aus sensiblen Bereichen zu beschaffen. Es ist dem NDB bekannt, dass der Offizier für die Führung der menschlichen Quellen Mobiltelefonanschlüsse benutzt. Insgesamt hat er vier Prepaid-Abonnemente für Mobiltelefone in der Schweiz gekauft. Um festzustellen, zu welchen Personen er mit diesen Telefonen Kontakt hat, ist es notwendig, die Verbindungsnachweise oder Randdaten dieser Mobiltelefonanschlüsse zu erheben.

*Buchstabe d* bezieht sich auf die schon heute in der Gesetzgebung über die Überwachung des Fernmeldeverkehrs für die Strafverfolgungsbehörden geregelte Ortung von Mobiltelefongeräten durch die Überwachung des Standortes und der Hauptstrahlungsrichtung der Antenne, mit der das Endgerät der überwachten Person momentan verbunden ist (vgl. Art. 16 Bst. b der Verordnung vom 31. Oktober 2001<sup>20</sup> über die Überwachung des Post- und Fernmeldeverkehrs). So kann ohne Zugriff auf das Gerät oder Platzierung eines Sensors bei der Person der ungefähre Standort eines Mobiltelefongerätes und dessen Bewegungen ermittelt werden. Weil

<sup>18</sup> SR 780.1

<sup>19</sup> Gemäss im Internet publizierter Statistik, siehe <https://www.li.admin.ch/de/themes/stats.html>

<sup>20</sup> SR 780.11

dabei auf Daten des Fernmeldeverkehrs zugegriffen werden muss und die Mitwirkung von Anbieterinnen von Fernmeldedienstleistungen notwendig ist, muss diese Massnahme dem Genehmigungsverfahren unterstehen.

*Buchstabe e* regelt den Einsatz von technischen Mitteln wie GPS-Geräten, mit welchen der Standort einer Person, eines Fahrzeugs oder einer anderen beweglichen Sache festgestellt werden kann. Es erfolgt eine Aufzeichnung des Bewegungsmusters oder eine Signalübertragung, mit der 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, wo ihre Verwendung seit Jahren gängige Praxis ist). Sie können diese 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 Zielobjektes, womit gezieltere Einsätze der Observationsteams ermöglicht werden).

Die Definition der einzusetzenden Geräte ist dabei offen, um künftige technische Entwicklungen nicht auszuschliessen.

*Buchstabe f* 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 23.

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 keine Kontakte zu aussenstehenden Personen, denen sie ihre Absichten und Vorbereitungen kundgeben. In solchen Kreisen können auch keine menschlichen Quellen eingesetzt werden, da diese Zellen keinen Zugang von aussen erlauben. Nur durch technische Überwachungsmittel können diejenigen Informationen beschafft werden, die zur Aufgabenerfüllung 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. 55).

*Buchstabe g* trägt der zunehmenden Verlagerung von sicherheitsbedrohenden Aktionen und Äusserungen ins Internet und dort in zugriffsgeschützte Bereiche Rechnung. Der NDB benötigt in Anbetracht der aus dem Internet erwachsenden Bedrohungen für die Sicherheit der Schweiz neue adäquate Mittel, um im Rahmen seiner präventiven Aufgabe die Netzwerke aufzuklären 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) in Fällen von Angriffen auf kritische Infrastrukturen.

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 und 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), chemische Industrie (z.B. Sondermüll), Telekommunikation (z.B. Radio und Fernsehen), Gesundheitswesen (z.B. medizinische Versorgung) oder das Finanz- und Versicherungswesen (z.B. Börsen). Ziffer 2 soll somit die Abwehr von unmittelbar drohendem oder bereits ganz oder teilweise eingetretenem Schaden während einem laufenden Angriff ermöglichen. Vorbehalten bleibt das Subsidiaritätsprinzip, indem der NDB nur im Sinne einer „ultima ratio“ aktiv wird. Hier muss der präventive Schutz der 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 (Zustimmung des Bundesverwaltungsgerichts), als auch politischer (Freigabe durch die Chefin oder den Chef des VBS) Genehmigung bedürfen.

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

Mit *Buchstabe h* schlagen wir neu vor, 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.

*Absatz 2* bestimmt, dass die vorstehenden Massnahmen verdeckt und ohne Kenntnis der betroffenen Personen durchgeführt werden. Das 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. 29) mit der Möglichkeit, gegen die Anordnung der Massnahmen Beschwerde zu führen (Art. 71).

## Art. 23 Grundsatz

*Absatz 1* knüpft den Einsatz genehmigungspflichtiger Beschaffungsmassnahmen zunächst an die (alternativen) Voraussetzungen des Vorliegens einer konkreten Bedrohung der inneren oder äusseren Sicherheit, mit Ausnahme des gewalttätigen Extremismus, oder der Wahrnehmung weiterer wesentlicher Landesinteressen auf Grund eines Bundesratsbeschlusses. Der Bundesrat legt in seinem Beschluss auch fest, ob genehmigungspflichtige Beschaffungsmassnahmen zum Einsatz kommen können. Das Bewilligungsverfahren richtet sich aber in jedem Fall nach Artikel 25ff., 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 wie bei einer konkreten Bedrohung der inneren oder äusseren Sicherheit nach Artikel 17 Absatz 2 Buchsta-

ben a-d müssen (kumulativ) folgende zusätzlichen Voraussetzungen erfüllt sein, damit eine bewilligungspflichtige Beschaffungsmassnahme eingesetzt werden kann:

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

Das sind zusätzliche, einschränkend umschriebene Anforderungen des verfassungsmässigen Verhältnismässigkeitsprinzips, die jenen im Strafprozessrecht nachgebildet sind (vgl. Art. 269 Abs. 1 der Schweizerischen Strafprozessordnung<sup>21</sup> (StPO)).

Beauftragte Drittstellen nach *Absatz 2* werden in der Praxis vor allem der Dienst ÜPF im EJPD für die mit Fernmeldeüberwachungen zusammenhängenden Massnahmen sein oder auch die Sicherheitsorgane der Kantone für den Einsatz von technischen Überwachungsgeräten oder bei Durchsuchungen.

#### *Art. 24* Anordnung von genehmigungspflichtigen Beschaffungsmassnahmen gegenüber Drittpersonen

Es kommt vor, dass eine Person, bei der die Voraussetzungen nach Artikel 23 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. 29).

Nicht zulässig ist die Überwachung einer Drittperson, die nach den Artikeln 171-173 StPO ein Zeugnisverweigerungsrecht besitzen, das heisst z.B. Geistliche, Rechtsanwälte, Medizinalpersonen und ihre Hilfspersonen oder Medienschaffende. Hier folgt das NDG ebenfalls den Regelungen der StPO.

#### *Art. 25* Genehmigungsverfahren

Das hier vorgeschlagene Genehmigungsverfahren ist zweistufig: Der NDB muss in einem ersten Schritt die Bewilligung 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. 26), die oder der vorgängig dazu den Sicherheitsausschuss des Bundesrates konsultiert.

Im Einzelnen gestaltet sich das Vorgehen wie folgt:

<sup>21</sup> SR 312.0

- Der NDB stellt dem Bundesverwaltungsgericht einen Antrag auf Einsatz einer genehmigungspflichtigen Beschaffungsmassnahme.
- Die Präsidentin oder der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts prüft den Antrag und entscheidet auf Genehmigung oder Ablehnung der beantragten Massnahme, bzw. kann sie oder er die Akten ergänzen lassen.
- Bei Genehmigung der Massnahme entscheidet die Chefin oder der Chef des VBS anschliessend über deren Freigabe.
- 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, die einzusetzenden Mittel und allfällige Schutzmassnahmen zur Wahrung der Persönlichkeitsrechte der überwachten Person oder von Dritten.

Die Genehmigung wird analog zu Artikel 274 Absatz 5 StPO für höchstens drei Monate erteilt, wobei sie jeweils um höchstens drei Monate verlängert werden kann. Erweist sich eine Verlängerung als notwendig, stellt der NDB einen Verlängerungsantrag mit den gleichen Angaben, wie sie für die Genehmigung notwendig sind (Abs. 5).

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 um zu verhindern, dass sie für Straffälle verwendet werden, in welchen keine vergleichbare strafprozessuale Ermittlungsmassnahme zulässig gewesen wäre (vgl. Art. 55 Abs. 3 und 4).

#### Art. 26 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 stark in die Grundrechte eingreifenden Massnahmen nicht nur nach rechtlichen, sondern auch nach politischen Gesichtspunkten beurteilt werden. 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.

## Art. 27 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 Artikel 22ff. grundsätzlich zuerst die Genehmigung durch das Bundesverwaltungsgericht und die Freigabe durch die Chefin oder den Chef des VBS, nach dessen vorgängiger Konsultation des Sicherheitsausschusses, einholen.

Artikel 27 sieht bei drohender Gefahr die Möglichkeit eines sofortigen Einsatzes der Massnahme durch den NDB vor. 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; oder
- nach dem Erteilen der Genehmigung durch das Bundesverwaltungsgericht die Freigabe ablehnen (vgl. Art. 29). 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. 28 Beendigung der 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, selbst wenn sie noch genehmigt wäre.

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. 29 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 EMRK und Artikel 13 BV.

Ist eine Operation, beziehungsweise ein zusammenhängender Vorgang möglicherweise mehrerer Beschaffungsmassnahmen bezüglich eines bestimmten Sachverhalts beendet, muss der NDB die Personen, die Ziel der Massnahme waren, und Drittpersonen, deren Anschlüsse allenfalls überwacht wurden, nach *Absatz 1* grundsätzlich innerhalb eines Monats über die Informationsbeschaffung unterrichten. 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. 22 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 eine Ausnahme nach Absatz 2 notwendig ist (z.B. weil der Fall an die Strafverfolgungsbehörden überwiesen und damit ein rechtliches Verfahren ausgelöst wird).

*Absatz 2 Buchstabe a* nimmt Bezug auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, der im Entscheid *Klass* gegen die Bundesrepublik Deutschland vom 6. September 1978 feststellte, dass eine nachträgliche Mitteilung den langfristigen Zweck einer Überwachung in Frage stellen und deshalb unter bestimmten 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 Art. 8 Abs. 2<sup>22</sup> 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.“*

*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 Talibankämpfer oder –kommandeur, dessen Mobiltelefon im Rahmen eines Entführungsfalls abgehört wurde, 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 könnten oder dass der Aufenthaltsort zwar bekannt ist, die betrof-

fene 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. 26).

## **5. Abschnitt: Zusammenarbeit und Quellenschutz**

### *Art. 30* Zusammenarbeit und Beauftragung in der Beschaffung

Heute sind staatliche und nichtstaatliche Akteure in den Bereichen Terrorismus, verbotener Nachrichtendienst, gewalttätiger Extremismus, verbotener Handel mit Waffen, chemischen, biologischen und nuklearen Massenvernichtungswaffen, sowie verbotener Technologietransfer global aktiv und halten sich nicht an zwischenstaatliche Grenzen oder Konventionen. Diese 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 zwecks Nachrichtenbeschaffung kann beispielsweise der Einsatz einer Quelle (an Stelle eines Mitarbeitenden 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 Informatikspezialisten bei besonders geschützten Datennetzwerken.

Der NDB hat sich bei allen Beauftragten nach Absatz 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 Mitarbeitenden.

### Art. 31 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 auch Unsicherheiten zwischen dem speziellen Ordnungsrecht und allfälligem widersprechenden allgemeinen Gesetzesrecht 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 Partnerdiensten, ohne deren umfassenden Schutz die Schweiz als unsicherer Partner 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 verurteilt und gesucht werden.

*Absatz 2* beschränkt den Schutz menschlicher Quellen (Art. 13) im Inland gegenüber Strafverfolgungsbehörden. Diese Personen erhalten keinen Quellenschutz, wenn sie selbst eines Officialdeliktes 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 allgemein gültige formellgesetzliche Definition. Es gibt auch keine generell gültigen Kriterien für schwere Straftaten. Vielmehr spielt der Kontext für die Qualifikation einer Straftat als schwer eine Rolle. Als Anhaltspunkt dafür, was als schwere Straftat gilt, kann immerhin die Definition in Artikel 11 Absatz 3 der Zwanganwendungsverordnung vom 12. November 2008<sup>23</sup> herangezogen werden:

*<sup>3</sup> 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 Entscheidungsinstanz vor.

## 6. Abschnitt: Beschaffung von Informationen über Vorgänge im Ausland

### Art. 32 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 zu Handen 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 Auslandsnachrichtendienstes (damaliger SND) nicht offenlegen wollte.

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

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

Die Nachrichtenbeschaffung im Ausland funktioniert hingegen nach etwas andern Regeln als diejenige im Inland. Der NDB setzt die Beschaffungsmassnahmen im Ausland in eigener Verantwortung ein, auch diejenigen, die im Inland bewilligungspflichtig wären (Art. 22ff.).

Die unterschiedliche Regelung der Inland- und Auslandsbeschaffung entspricht einer Praxis, die für die meisten Nachrichtendienste der Welt Gültigkeit hat und sich im Grunde aus der Tatsache ergibt, dass staatliche, nachrichtendienstliche Informationsbeschäftigungen 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 zu berücksichtigen,

- dass auch bei der Informationsbeschaffung im Ausland der Kerngehalt der Grundrechte respektiert werden soll (Abs. 3);
- dass die Beschaffungsaktivitäten betreffend Vorgänge im Ausland zu Handen der Aufsichts- und Kontrollorgane eng dokumentiert werden (Abs. 4); und

- dass die Informationsbeschaffung im Ausland der Kontrolle durch das VBS durch den Bundesrat und schliesslich durch die GPDel unterliegt (vgl. Art. 66ff.).

*Absatz 1* statuiert den Grundsatz, dass Beschaffungsaktivitäten im Ausland verdeckt durchgeführt werden. Das ist notwendig, da sie ansonsten durch betroffene Staaten oder Akteure verhindert werden und sowohl Mitarbeitende 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. Das gilt insbesondere für die allfällige Anwendung von bewilligungspflichtigen Beschaffungsmassnahmen (4. Abschnitt). Davon ausgenommen ist das Eindringen in Computersysteme und –netzwerke (Art. 22 Abs. 1 Bst. g), sofern sich diese Systeme und Netzwerke im Ausland befinden. Hier wäre eine Genehmigungspflicht unverständlich, da derselbe Eingriff genehmigungsfrei wäre, wenn er von einem Standort jenseits der Grenze ausgeführt würde.

Der NDB verwendet verdeckte Beschaffungsmassnahmen im Ausland in eigener Verantwortung, auch solche, die nach Artikel 22ff. im Inland bewilligungspflichtig wären. Der Grund für die gegenüber der Inlandbeschaffung abweichende Lösung beim Einsatz der Beschaffungsmassnahmen liegt neben den oben erwähnten Gründen zudem darin, dass die mit der Beschaffung von Auslandsnachrichten befassten Mitarbeitenden 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, in einer abschliessenden Aufzählung ohne besondere Genehmigung zu regeln. Dies weil Schweizer Gerichte im Regelfall weder die jeweiligen Verhältnisse vor Ort kennen können, noch sich innert nützlicher Frist die für eine verantwortungsvolle Entscheidungsfindung notwendigen 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.

Dies bedeutet indessen nicht den Wegfall einer wirksamen Kontrolle. Im Gegenteil: *Absatz 4* verpflichtet den NDB, die gesamte Beschaffung von allen 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.

Die im Ausland eingesetzten Mitarbeitenden des NDB sind einem erhöhten Risiko ausgesetzt und bewegen sich auch in Kriegs- und in Krisengebieten, zum Teil unter Legenderungen und Tarnidentitäten. Der Bundesrat schlägt in *Absatz 5* deshalb ihre Unterstellung unter die Militärversicherung vor.

Die in *Absatz 6* vorgesehenen Schutzmassnahmen können in Form von technischen Ausrüstungen, aber auch von Legenderungen und Tarnidentitäten oder operationeller Unterstützung bestehen, z.B. dem Einsatz von Gegenobservationen zur frühzeitigen Erkennung von Gefährdungen im Umfeld eines Einsatzes.

### *Art. 33* Funkaufklärung

Das Parlament hat im Rahmen der Revision BWIS II im ZNDG mit Artikel 4a eine neue gesetzliche Bestimmung geschaffen, welche die nachrichtendienstliche Funkaufklärung erstmals auf dieser Stufe regelt. Diese Bestimmung trat nach der Anpassung der Verordnung über die elektronische Kriegführung 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 weiterer wesentlicher Landesinteressen im direkten Auftrag des Bundesrates (vgl. Art. 1 Abs. 3 und Art. 62) in die möglichen Voraussetzungen für den Einsatz der Funkaufklärung aufgenommen.

Die Funkaufklärung ist auf das Ausland ausgerichtet, das heisst sie darf nur Funksysteme erfassen die sich im Ausland befinden. 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 nur anonymisiert an den NDB weiterleiten, sofern sie nicht auf eine konkrete Gefährdung der inneren Sicherheit hinweisen (Abs. 5). Das ZNDG verweist hier auf die weitere Bearbeitung nach den Regelungen des BWIS. Unter dem NDG sind darunter Bedrohungen nach Artikel 4 Absatz 1 Buchstabe a zu verstehen.

Die Funkaufklärung wird heute schon von einer Unabhängigen Kontrollinstanz UKI kontrolliert. Auch hier übernimmt der Bundesrat die entsprechende Regelung aus dem ZNDG (Art. 4b) weitgehend unverändert in Artikel 66 NDG.

Damit übernimmt das NDG vollständig die bisherige rechtliche Regelung und Praxis 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, massgeblich beteiligt. Die vorliegende Bestimmung des NDG wie auch der folgende Abschnitt zur Kabelaufklärung wurden deshalb wiederum unter Beteiligung von Prof. Biaggini erarbeitet.

## **7. Abschnitt: Kabelaufklärung**

### *Art. 34* Allgemeines

Neben der auch in der Schweiz schon heute praktizierten Funkaufklärung gewinnt international die Kabelaufklärung an Bedeutung. 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 etwas ab, Erkenntnisse aus der Funkaufklärung zu gewinnen. Der Vorentwurf orientiert sich deshalb teilweise an einer entsprechenden Gesetzgebung, die Schweden 2008 erlassen hat (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.

Die Kabelaufklärung dient wie die Funkaufklärung der Informationsbeschaffung über das Ausland und ist deshalb nicht als genehmigungspflichtige Beschaffungsmassnahme 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 von schweizerischen Anbieterinnen von Fernmeldedienstleistungen durchgeführt werden, welchen eine rechtsgültige Anordnung für das Weiterleiten der entsprechenden Datenströme an die ZEO übergeben werden muss. Da hier ein kontradiktorisches 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. 25). Die Bearbeitung der Daten erfolgt aber anders als bei den genehmigungspflichtigen Beschaffungsmassnahmen nicht in separaten Systemen, sondern wie die Erkenntnisse aus der Funkaufklärung im Restdatenspeicher und im IASA NDB (Art. 42ff.).

Bei der Kabelaufklärung werden bestimmte Datenströme auf internationalen Fernmeldekabeln erfasst und ähnlich wie bei der Funkaufklärung nach Inhalten abgesehen, triagiert und der Auswertung zugeführt. Im Gegensatz zur Fernmeldeüberwachung im Inland als genehmigungspflichtige Beschaffungsmassnahme ist die Kabelaufklärung ein Mittel der Auslandsaufklärung und ist nicht darauf ausgerichtet, den gesamten Fernmeldeverkehr von bestimmten Anschlüssen zu erfassen. Dies ist technisch nicht in der gleichen Art möglich, da sich die Zielobjekte im Ausland befinden.

Die Schweiz hat bisher noch keine Erfahrungen mit diesem Aufklärungsmittel, da hierzu keine rechtlichen Grundlagen bestehen.

Der durchführende Dienst nach *Absatz 1* ist wie bei der Funkaufklärung das Zentrum für elektronische Operationen ZEO der Armee. 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.

*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 und Empfänger 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 definiert. Diese sollen möglichst präzise gefasst sein, damit die Datenerfassung möglichst geringe Eingriffe in die Privatsphäre von Personen verursacht. Das heisst, dass beispielsweise die Suche nach konkreten Personalien von ausländischen Ter-

rorverdächtigen oder der Fernmeldeanschlüsse, die diese verwenden, wirkungsvoller und schonender ist als die Verwendung eines trivialen Suchwortes wie „Al Qaida“ 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. 35 / 36* Genehmigungspflicht und Genehmigung des Auftrags zur Kabelaufklärung

Diese Artikel regeln analog zu den genehmigungspflichtigen Beschaffungsmassnahmen die Genehmigung der Aufträge für die Kabelaufklärung. Weil hier Fernmeldeproviderinnen Anordnungen für die Weiterleitung bestimmter Datenströme zugestellt werden müssen und kein Widerspruchsverfahren durch die betroffenen Personen möglich ist, ist eine richterliche Überprüfung notwendig.

Der Antrag nach *Artikel 36 Absatz 1* umfasst auch die Kategorien von Suchbegriffen, nach welchen die Daten zu Händen 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 Triage in einen Auftrag mehr Zeit erfordert als z.B. die umfassende Zuleitung an den NDB aller Kommunikationen bei einer Fernmeldeüberwachung nach *Artikel 22 Absatz 1 Buchstabe a*. Für die Verlängerungen gilt dann dieselbe Frist wie bei den genehmigungspflichtigen Beschaffungsmassnahmen von drei Monaten.

#### *Art. 37* Vollzug der Kabelaufklärung

Die Durchführung gleicht dem Verfahren bei der Funkaufklärung, mit der Ausnahme, dass der durchführende Dienst bei der Kabelaufklärung die Signale der Fernmeldeeinrichtungen nicht selbst erfasst (mit Antennen), 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 (siehe 4. Kapitel). Wie bisher kann das ZEO die weitergeleiteten Daten aber auch mit technischen oder inhaltlichen Erläuterungen, Zusammenfassungen oder Übersetzungen zu Händen des NDB versehen.

*Art. 38*            **Verpflichtungen der Betreiberinnen von leitungsgebundenen Netzen und der Anbieterinnen von Telekommunikationsdienstleistungen**

Da wie bereits erläutert die Kabelaufklärung nur mit Beteiligung der Anbieterinnen von Fernmeldedienstleistungen und der Betreiberinnen von leitungsgebundenen Netzen betrieben werden kann, legt Artikel 38 deren Verpflichtungen in diesem Rahmen fest. Verpflichtet sind dabei nur Betreiberinnen, die öffentliche Leistungen im Sinne des 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 Auftrages 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 Fernmeldedienstleistungen und Betreiberinnen von leitungsgebundenen Netzen.

Eine Beteiligung des Dienstes ÜPF im EJPD ist dabei nicht notwendig, da es sich bei der Kabelaufklärung nicht um eine von diesem angebotene Überwachungsart gemäss 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 erst erhoben werden, wenn die entsprechenden gesetzlichen Grundlagen vorliegen.

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 erfordert. Diese werden in den ordentlichen Personalplänen beantragt werden.

## **4. Kapitel: Datenbearbeitung und Archivierung**

### **1. Abschnitt: Grundsätze und Datenbearbeitung in den Kantonen**

#### *Einleitende Bemerkungen*

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

Terroristische Anschläge, Spionageaktivitäten, gewaltextremistische Aktionen usw. werden typischerweise verdeckt vorbereitet und so lange wie möglich geheim gehalten.

ten. Sie können aber zu beträchtlichen Schäden führen, weshalb ihre Früherkennung und Abwehr zentral ist. Deshalb muss die Informationsbearbeitung bereits zu einem Zeitpunkt erfolgen, an 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.

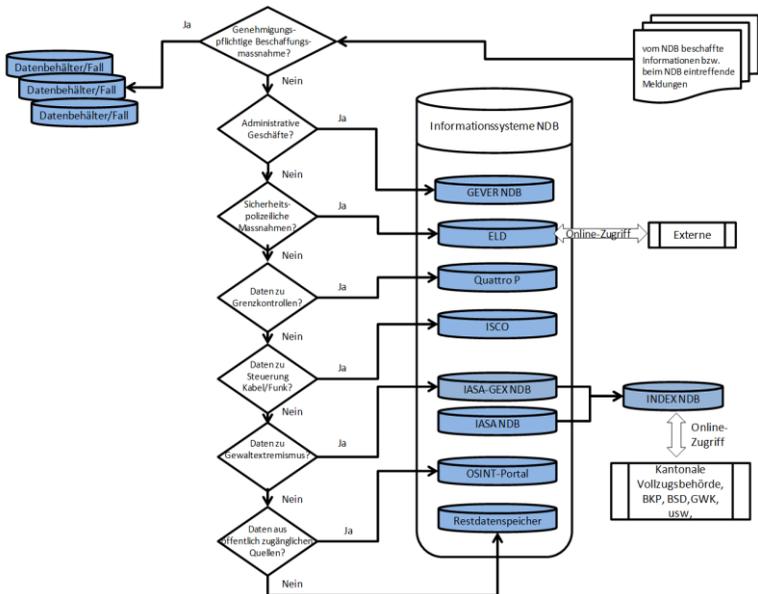
Das vorliegende Gesetz verzichtet konsequent auf die nicht mehr zeitgemässe Trennung zwischen innerer und äusserer Sicherheit, so dass diese Unterscheidung auch bei der Datenbearbeitung durch den NDB keine bestimmende Rolle spielen kann.

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 BWIS und 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 einen Verbund von Informationssystemen abgelegt werden. Der NDB kann nicht wahllos Daten sammeln und aufbewahren. Voraussetzung ist immer ein genügender Bezug zu seinen Aufgaben nach diesem Gesetz. Weiter ist die Einhaltung der Datenbearbeitungsschranke bezüglich der Ausübung der politischen Rechte zu beachten (Art. 3 Abs. 5 bis 8). Schliesslich wird sichergestellt, dass die Daten bereits vor der Ablage auf Erheblichkeit und Richtigkeit überprüft werden. Ebenso erfolgt diese Prüfung, bevor Personendaten eine Aussenwirkung entfalten, indem sie innerhalb eines Produkts des NDB (z.B. Analysebericht, Meldung an Partnerdienst, Lagebeurteilung) verwendet werden.

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

Die verschiedenen Informationssysteme des NDB erlauben eine differenzierte Regelung der Datenhaltung. Während die Datenbearbeitung beispielsweise im Bereich 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 Datenbearbeitungsaufgaben 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. 39 Grundsätze

Die in Artikel 39 festgehaltenen Grundsätze gelten für alle Informationssysteme des NDB. Damit wird ein einheitlich hoher Standard der Datenbearbeitungsqualität sichergestellt, egal in welchem System Personendaten gespeichert sind. Die Systeme können die Daten in Form von Texten, Ton oder Bild oder anderen geeigneten Formaten enthalten.

Der NDB ist zur Auftrags Erfüllung immer wieder auf die Bearbeitung besonders schützenswerter Personendaten, wie z.B. die Religionszugehörigkeit bei fundamentalistisch motivierten Terroristen, die Verbüssung von Haftstrafen durch Verurteilte oder den Gesundheitszustand von Identifikationsfiguren oder ausländischen Politikern angewiesen. Er erstellt und bearbeitet Persönlichkeitsprofile, z.B. zur Einschätzung der Bedrohung durch gewaltextremistische Einzeltäter oder Gruppen. *Absatz 1* schafft für diese Datenbearbeitungen die notwendige formellgesetzliche Grundlage.

In Abweichung zu den üblichen Datenschutzaufgaben muss der NDB gemäß *Absatz 2* auch als unrichtig erkannt und entsprechend bewertete Daten aufbewahren dürfen. Bei der Beurteilung von nachrichtendienstlichen Informationen geht es auch immer um das Erkennen von Desinformation und Falschinformation. Solche Informationen lassen Absichten von Informationsproduzenten und -lieferanten erkennen. Einmal erkannte Des-, respektive Falschinformation muss auch in Zukunft als solche bekannt und vorhanden sein, um keine späteren Fehlurteilungen 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, Vertrauenswürdigkeit oder der Absichten einer menschlichen Quelle oder eines Partnerdienstes.

Die Informationssysteme des NDB bilden einen Verbund; sie dienen alle dem Zweck der Erfüllung der gesetzlichen Aufgaben des NDB. Dabei müssen Daten oft für die Auftragsbefreiung in ein anderes System überführt werden. Der Analytiker, 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 vorgesehenen Informationssystem IASA NDB nur dann durchführen und belegen können, wenn er die benötigten 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 Anwendern zur Verfügung steht. Dort wird sie weiterhin regelmässig auf ihre Erheblichkeit und Richtigkeit überprüft (vgl. Art. 40, 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 Auswerteprogrammen.

#### *Art. 40*            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 dem differenzierten Datenerfassungsmodell gezielt eingesetzt:

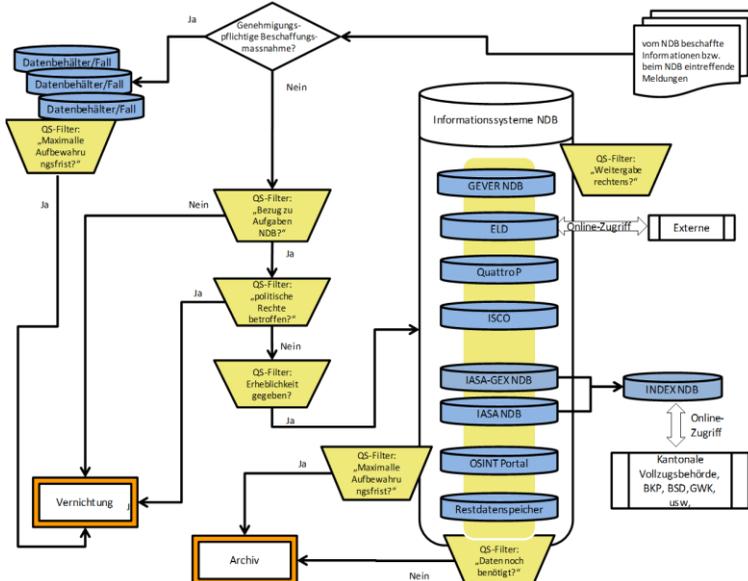
- Eine unmittelbare und lückenlose Überprüfung durch die interne Qualitätssicherungsstelle ist bei den Datenbearbeitungen im Bereich des Gewaltextremismus (Abs. 5 Bst. a) sowie bei der Erfassung kantonaler Berichte im INDEX NDB (Abs. 5 Bst. b) sichergestellt. Während in den Bereichen unerlaubter Nachrichtendienst, Proliferation oder Terrorismus zumeist langjährige Entwicklungen zu beobachten sind, ist im Bereich des Gewaltextremismus mit viel kürzeren Halbwertszeiten der Datenqualität zu rechnen. 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 Datenbearbeitungsaufgaben 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 mit-

tels Ausbildung, Vorgaben und Kontrollen für die korrekte Umsetzung der vorgeschriebenen Datenbearbeitungsfilter. Es ist vorgesehen, dass Mitarbeitende 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 jenen der Aufsichtsorgane (Art. 65ff.). 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 der Meldung als Ganzes.

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 Daten werden regelmässig daraufhin überprüft, ob sie für die Erfüllung der Aufgaben nach diesem Gesetz noch benötigt werden;
- Ausgangstriage: nur wenn die Datenbearbeitung rechters ist, dürfen die Personendaten eine Aussenwirkung entfalten (vgl. Art. 54);
- 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 Erheblichkeit und Richtigkeit der Personendaten. Diese Beurteilung erfolgt für das nicht nach Personenobjekten geordnete System Restdatenspeicher 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. 4 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, verbotenen Nachrichtendienst, Proliferation, Angriffen auf kritische Infrastrukturen oder sicherheitspolitisch bedeutsamen Vorgängen aufweisen. Des Weiteren ist die Bearbeitungsschranke zum Schutz der politischen Rechte (Art. 3 Abs. 5-8) zu beachten.

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. 59).

#### *Art. 41*            Datenbearbeitung in den Kantonen

*Absatz 1* liegt folgendes Konzept zu Grunde: 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. Artikel 46). 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.

Daten nach *Absatz 2* bearbeiten 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 gewaltextremistische Ausschreitungen zu befürchten, so bearbeitet sie der NDB auch unter diesem Gesichtspunkt. Verläuft die Kundgebung tatsächlich gewalttätig, so bearbeitet der NDB diese Informationen aus dem Gesichtspunkt des gewalttätigen Extremismus nach diesem Gesetz, während die kantonalen Behörden die Straftaten wie Sachbeschädigung, Landfriedensbruch oder Körperverletzung in eigener Kompetenz bearbeiten. Wegen den 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. auf Grund von entsprechendem Verhalten bei Befragungen.

## 2. Abschnitt: Nachrichtendienstliche Informationssysteme

### Art. 42 Informationssysteme des NDB

Artikel 42 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<sup>24</sup> 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<sup>25</sup> 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 fest nach der ersten Erfassung und danach alle drei Jahre für die wiederkehrende Überprüfung bis zur maximalen Aufbewahrungsdauer. 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.

Im weiteren wird der NDB gemäss den allgemeinen datenschutz- und informationsschutzrechtlichen Vorgaben zu allen Informationssystemen Bearbeitungsregelungen 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. 43 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 Datenart vorgesehenen System zu. Den Systemen IASA NDB und INDEX NDB werden keine Daten direkt zugewiesen. IASA dient den Auswerterinnen und Auswertern des NDB zum Zusammentragen, Auswerten und Dokumentieren der für die Produktion notwendigen Daten und Erkenntnisse. Der INDEX NDB enthält von Seiten des NDB vor allem die Identifi-

<sup>24</sup> SR 361

<sup>25</sup> SR 121.2

kationsdaten für Personen, Organisationen, Gegenstände und Ereignisse, die aus den Systemen IASA NDB und IASA-GEX NDB in den INDEX NDB kopiert werden.

#### *Art. 44* Informations- und Analysesystem Auswertung (IASA NDB)

Artikel 44 bildet die formellgesetzliche Grundlage für 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. 45). IASA NDB löst damit weitestgehend die heutigen Systeme ISIS und ISAS ab.

Verantwortlich für das Erfassen und periodische Überprüfen der im IASA gespeicherten Daten sind die Auswerterinnen und Auswerter des NDB in ihren jeweiligen Spezialgebieten. Die interne Qualitätssicherungsstelle führt zusätzlich regelmässig Stichproben durch, um die gesetzeskonforme Bearbeitung zu kontrollieren (vgl. Art. 40).

#### *Art. 45* Informations- und Analysesystem Auswertung Gewaltextremismus (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 3 Absatz 5 NDG der Informationsbeschaffung und -bearbeitung entzogenen politischen Betätigung grösser ist. Sie werden deshalb in einem besonderen Informationssystem 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. 40 Abs. 5 Bst. a).

Der Bundesrat legt gemäss Artikel 61 Absatz 1 Buchstabe c jährlich fest, welche Gruppierungen, als gewaltextremistisch einzustufen sind.

#### *Art. 46* INDEX NDB

Der INDEX NDB dient einerseits der Feststellung, ob der NDB Daten zu einer bestimmten Person, Organisation, einem Gegenstand oder einem Ereignis bearbeitet. Alle im IASA NDB und IASA GEX NDB erfassten Personen sind hier abrufbar. Konkret werden hier die wichtigsten Identifikationsdaten erfasst, wie beispielsweise bei Personen Namen, Geburtsdatum, 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 mit sicherheits- und kriminalpolizeilichen Tätigkeiten. Heute erfolgt dies, indem Amtsstellen ausserhalb des NDB einen auf die Identifikationsdaten eingeschränkten direkten Zugriff auf das System ISIS haben. Stellen ausserhalb des NDB und der kantonalen Vollzugsbehörden haben keinen Zugang zu über die Identifikationsdaten hinausgehenden Informationen. Sie müssen mit dem NDB in Kontakt treten, um allenfalls weitere Daten auf dem Weg der formellen Zusammenarbeit und Datenweitergabe (Art. 54ff.) 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. Sie bearbeiten hier die Daten im Vorfeld zu einem Bericht an den NDB. Der Index erlaubt ihnen weiter die Übersicht über die Aufträge des Bundes und die Ablage. Mit dieser Zentralisierung auf Bundesebene aller im Rahmen dieser Vorlage erfolgenden Datenbearbeitungen, wird eine einheitliche Regelung und Kontrolle sichergestellt.

#### *Art. 47*            Geschäftsverwaltung NDB (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. 48*            Elektronische Lagedarstellung (ELD)

Artikel 48 übernimmt von Artikel 10a 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.

Zu *Absatz 3* hat im Rahmen von BWIS II der ausnahmsweise Zugang von Privaten oder ausländischen Behörden zu erheblichen Diskussionen geführt. Die bisherige Praxis hat die restriktive Anwendung dieser Bestimmung durch den NDB bestätigt: Bisher wurden keine solchen Zugänge gewährt, weil keine entsprechenden Situationen vorlagen. Der Bundesrat ist aber nach wie vor überzeugt, dass die Schweiz als Gastgeber 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 Gefährdungspotential 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

gibt nur zu denjenigen Daten Zugriff, die für diese besondere Bedrohungsabwehr benötigt werden.

#### *Art. 49*            Zugangsportal öffentliche Informationsquellen (OSINT-Portal)

Artikel 49 bildet die formellgesetzliche Grundlage für das OSINT-Portal, das System des NDB zur Nutzung der öffentlich zugänglichen Daten. Eine Speicherung z.B. von Internet-Daten 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 grundsätzlich jedermann zugängliche Daten handelt, 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.

#### *Art. 50*            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).

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).

Der Bundesrat bestimmt gemäss *Absatz 4* jährlich den Umfang der Kontrollen, das heisst die massgebenden Herkunftsländer und allfällige Einschränkungen auf bestimmte Personenkategorien (z.B. nur Männer oder nur Inhaber von bestimmten Arten von Pässen). Das Vorgehen ist vergleichbar mit dem Festlegen nach Artikel 18 Absatz 4 der Vorgänge und Feststellungen, die 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. 51*            Informationssystem Kommunikationsaufklärung (ISCO)

Das System ISCO (Informationssystem COMINT) 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. 33ff.). 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 Unabhängigen Kontrollinstanz UKI, vgl. Art. 67) als Basis für ihre Tätigkeiten.

Zugriff auf ISCO haben nur sehr wenige Mitarbeitende 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. 52).

#### *Art. 52* Restdatenspeicher

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

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 Erkennungskriterien der Erheblichkeit (Bezug zu einem Aufgabengebiet des NDB, Respektierung der Bearbeitungsschranken von Art. 3 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 Dokumentes überprüft.

### **3. Abschnitt: Daten aus genehmigungspflichtigen Beschaffungsmassnahmen**

#### *Art. 53*

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, welche 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 konspirative Elemente in der Kommunikation anwendet, um diese zu schützen. 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 Internet-Kommunikationen oder beim Eindringen in Computersysteme auch Schadsoftware (Viren, Trojaner) auftauchen können. Diese sollten nicht in die Systeme des NDB eingeschleppt werden.

Artikel 53 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.

Entsprechend schränkt *Absatz 3* den Zugang zu diesen Daten auf diejenigen Personen ein, welche der unmittelbaren Durchführung der Massnahme und der Auswertung ihrer Ergebnisse beauftragt sind. Dies werden in der Regel die zuständigen Sachbearbeitenden der Beschaffung und Auswertung sein, welche den jeweiligen Fall bearbeiten.

#### **4. Abschnitt: Besondere Bestimmungen über den Datenschutz**

##### *Art. 54* Überprüfung vor der Weitergabe

Nicht nur die besonders 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. 55* Weitergabe von Personendaten an inländische Behörden

Damit der der NDB seinen Auftrag erfüllen kann, muss er Personendaten an politische Behörden, Strafverfolgungs-, Justiz- oder Sicherheitsbehörden weiterleiten können. Die Regelung entspricht weitgehend geltendem Recht von Artikel 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.

##### *Art. 56* 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). Das würde die meisten aussereuropäischen Länder von der Zusammenarbeit mit dem NDB ausschliessen, falls nicht im Einzelfall die restriktiven Ausnahmen von Artikel 6 Absatz 2 DSG zur Anwendung kommen könnten. Dies würde den NDB von wichtigen Informationsquellen gerade in Krisenregionen ausschliessen.

Schon das BWIS stellt deshalb besondere Regelungen für die nachrichtendienstliche Zusammenarbeit und Weitergabe von Personendaten mit dem Ausland 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.

*Absatz 2 Buchstabe d* betrifft die schon in Artikel 10 Absatz 1 Buchstabe d erwähnten Unbedenklichkeitsanfragen oder Clearings zu Gunsten 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. 57* 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 Auskunftsgesuches, beim Einholen von Auskünften über natürliche oder juristische Personen muss der NDB gegenüber der befragten Person natürlich sagen können, über welche Person er eine Auskunft braucht und in welchem Zusammenhang. Die Bestimmung entspricht dem heutigen Artikel 17 Absatz 3 BWIS.

#### *Art. 58* Auskunftsrecht

Für das Auskunftsrecht übernimmt der Entwurf die vom Parlament im Rahmen der BWIS-Revision vom 23. Dezember 2011 („BWIS II-reduziert“) beschlossene Lösung, die sich an das BPI anlehnt. Das NDG übernimmt dabei den am 16. Juli 2012 in Kraft getretenen Artikel 18 BWIS in seiner neuen Fassung weitgehend.

Im Rahmen der Beratung von BWIS II hatte der Bundesrat in der Diskussion um die Neugestaltung des Auskunftsrechts noch beantragt, das DSG integral anzuwenden. Da sich das Parlament jedoch bewusst für die Lösung nach BPI entschieden hat, erachtet es der Bundesrat nicht als sinnvoll, erneut eine andere Auskunftsregelung zu unterbreiten.

Das Verfahren 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 Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gelangen, der sinngemäss das frühere Verfahren der indirekten Auskunft durchführt.

Als Abweichung zur aktuellen BWIS-Regelung schlägt der Bundesrat vor, in *Absatz 9* auf die ursprüngliche Formulierung im BPI zurück zu kommen. 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 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 in der Regel jedoch nicht erbringen, weil ihm über diese Personen gerade keine Informationen vorliegen. Damit wird die Regel von Absatz 2 Buchstabe c ausgehebelt, welche besagt, dass bei nicht verzeichneten

Personen die Auskunft aufgeschoben wird. Der Bundesrat erachtet deshalb das Vorgehen gemäss BPI als sachlich richtiger.

## **5. Abschnitt: Archivierung**

### *Art. 59*

Die Daten und Akten des NDB unterstehen grundsätzlich dem Bundesgesetz vom 26. Juni 1998<sup>26</sup> über die Archivierung (BGA) und werden deshalb nach Ablauf ihrer Aufbewahrungsdauer in (teilweise besonders gesicherten) Räumen des Bundesarchivs aufbewahrt und nach den Grundsätzen des Archivwesens verwaltet. Eine Ausnahme besteht bereits heute in Bezug auf Daten und Akten aus dem direkten Verkehr mit ausländischen Sicherheitsdiensten. Diese stehen immer unter dem international üblichen Vorbehalt, dass ihre Weitergabe und Archivierung nur mit der ausdrücklichen Zustimmung des ausländischen Datenherrs zulässig ist. Deshalb soll der Bundesrat die Aufbewahrung und Vernichtung dieser Daten und Akten im Sinne der aktuellen Rechtsgrundlage (Artikel 28 Absatz 2 V-NDB) in einer Verordnung regeln.

## **5. Kapitel: Dienstleistungen**

### *Art. 60*

Der NDB ist grundsätzlich wie jede andere Amtsstelle berechtigt und verpflichtet Amtshilfe zu leisten in den Bereichen, 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. Die Sicherheitsorgane des Bundes und internationaler Organisationen greifen auf die Kompetenzen des NDB im Bereich Abhörsicherheit und Informationsschutz zurück. Der NDB berät die Beschaffungsorgane des Bundes zu den Themen Tresore und Schliesstechnik. Ausländische Partnerdienste 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.

<sup>26</sup> SR 152.1

- 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.

Der Bundesrat erachtet es als richtig, für diese Unterstützungen eine ausdrückliche gesetzliche Grundlage zu schaffen.

## **6. Kapitel: Politische Steuerung, Kontrolle sowie Rechtsschutz**

### **1. Abschnitt: Politische Steuerung und Tätigkeitsverbot**

#### *Art. 61* Politische Steuerung durch den Bundesrat

Der NDB ist ein Instrument, das in besonderem Masse 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 61 nimmt deshalb verschiedene Elemente der bisherigen Gesetzgebung auf und fasst sie in einer zentralen Bestimmung über die politische Steuerung zusammen.

*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.

Gegenwärtig ist der Grundauftrag auf Stufe Verordnung geregelt (Art. 2 Abs. 2 V-NDB). Er ist auf Grund seiner Bedeutung und seines Inhalts „geheim“ klassifiziert.

*Buchstabe b* verweist auf die Beobachtungsliste, die in Artikel 63 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 bewilligungspflichtigen Massnahmen nach Art. 22ff. durchgeführt werden. Weiter werden die Daten betreffend die gewaltextremistischen Gruppierungen im Rahmen der Datenbearbeitung des NDB im speziellen Informationssystem IASAGEX NDB abgelegt (Art. 45). Gleichzeitig berichtet ihm der NDB über die Anzahl von Personen des gewaltextremistischen 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 Partnerdiensten des NDB betrieben würde, müsste hingegen gemäss *Absatz 2* 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. 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.

#### *Art. 62*            Wahrung weiterer wesentlicher Landesinteressen

Dieser Artikel knüpft an Artikel 1 Absatz 3 an und legt das Verfahren fest, mit welchem der NDB in besonderen Lagen mit Massnahmen zur Wahrung weiterer 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 tätig werden darf.

#### *Art. 63*            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. 60 Abs. 1 Bst. b). Seit dem 11. September 2001 geht die internationale Gemeinschaft verstärkt gegen den Terrorismus vor. Durch den Einbezug der internationalen Listen (Revision BWIS II-reduziert vom 23.12.2011) 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 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 Resolution Nr. 1267 verbunden. Im Gegensatz zur Liste des UN-Sicherheitsrates werden in die Beobachtungsliste auch keine Einzelpersonen aufgenommen. Und schliesslich bleibt dank dem jährlichen Genehmigungsverfahren durch den Bundesrat der Handlungsspielraum gewahrt, eine Gruppierung von der Liste zu entfernen. Die Aufnahme einer Organisation, Gruppierung (oder Person) auf eine internationale Liste führt also nicht dazu, dass sie automatisch auch in die schweizerische Beobachtungsliste überführt werden muss.

Bei der Beobachtungsliste gilt die Bearbeitungsschranke nach Artikel 3 Absatz 5 (politische Betätigung und Ausübung von Grundrechten) nicht (vgl. Art. 3 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.

#### *Art. 64*            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 und äusseren Sicherheit nicht ein. Diese Befugnis des Bundesrates bleibt in den Fällen parallel weiter bestehen, die durch das Gesetz nicht geregelt sind.

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 Voraussetzungen dafür weiterhin erfüllt sind. Mit Hilfe dieser neuen Bestimmung könnte der Bundesrat beispielsweise Tätigkeitsverbote für Ableger von Terrororganisationen verfügen. Für die Al Qaida besteht gegenwärtig eine Ende 2014 auslaufende Verordnung der Bundesversammlung, die Al Qaida 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 auf Grund 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.

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. In Abweichung zur heutigen Regelung im BWIS sollen aber alle Departemente 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 so 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 71 beim Bundesverwaltungsgericht angefochten und anschliessend an das Bundesgericht weitergezogen werden.

## **2. Abschnitt: Kontrolle und Aufsicht des Nachrichtendienstes**

### *Einleitende Bemerkungen*

Die Artikel 65 bis 69 enthalten in aufsteigender Reihenfolge die Kaskade der Aufsichts- und Kontrollvorschriften:

1. Selbstkontrolle durch den NDB
2. Aufsicht und Kontrolle durch das VBS
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. 4b ZNDG, Art. 25ff. BWIS und Art. 31ff. V-NDB).

Die unabhängige Kontrollinstanz (UKI, Artikel 67) stellt die Rechtmässigkeit der Funkaufklärung über das Ausland nach Artikel 33 sicher.

### *Art. 66* Aufsicht durch das Departement

Die departementsinterne, nachrichtendienstliche Aufsichtsinstanz (heute Nachrichtendienstliche Aufsicht, NDA) wird neu auf Gesetzesstufe geregelt (Abs. 2), weil ihr erweiterte Befugnisse zugeteilt werden sollen. So soll auch ihre Kontrolltätigkeit bei den kantonalen Vollzugsbehörden gesetzlich geregelt werden (Abs. 3). Dies gilt für jene Bereiche, in denen die Kantone gestützt auf Bundesrecht Informationen beschaffen (vgl. Art. 73). Auf diese Weise wird die Kontroll- und Steuerungsaufgabe des VBS nach Absatz 1 ergänzt.

### *Art. 67* Unabhängige Kontrollinstanz für die Funkaufklärung

Die Regelung über die unabhängige Kontrollinstanz (UKI) entspricht wie jene über die Funkaufklärung (Art. 33) der am 1. November 2012 in Kraft getretenen Rege-

lung, welche das Parlament direkt im ZNDG verankert hat (Art. 4b ZNDG). Es handelt sich heute um eine verwaltungsinterne Kommission. 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. 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 Fernmeldedienstleisterinnen in der Schweiz erfordert. Dies ist bei der Funkaufklärung, die von den Bundesbehörden (ZEO und NDB) selbständig vollzogen werden kann, nicht der Fall.

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

Als einziger Unterschied zu Artikel 4b ZNDG figuriert die Amtsdauer der UKI nicht in Absatz 1, sondern in Absatz 4, da es sich eher um eine Einzelheit des Vollzugs handelt.

#### *Art. 68* 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. 69* 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 der Eidgenössischen Räte. Diese Kontrolle umfasst sowohl die Tätigkeiten des NDB wie diejenigen der kantonalen Vollzugsbehörden. Eine Zweiteilung der Oberaufsicht durch die kantonalen Parlamente einerseits und durch das eidgenössische Parlament andererseits ist im Rahmen dieser Vorlage nicht vorgesehen.

Der Bundesrat ist der Auffassung, dass der Bundesgesetzgeber mit der Schaffung der Geschäftsprüfungsdelegation für die Überwachung der Tätigkeit im nachrichtendienstlichen Bereich und der Zuweisung von besonderen Kompetenzen an diese Delegation in Artikel 53 des Bundesgesetzes vom 13. Dezember 2002<sup>27</sup> über die Bundesversammlung eine abschliessende Regelung der parlamentarischen Oberaufsicht getroffen hat. Es wäre nicht konsequent, wenn der Bundesgesetzgeber den Kantonen ohne besondere Auflagen parallele Kompetenzen auf kantonaler Ebene einräumen würde. Die kantonalen Sicherheitsorgane werden immer im direkten

<sup>27</sup> SR 171.10

Vollzug des Gesetzes zu Handen der Bundesorgane tätig und nicht im originären Vollzugsinteresse der Kantone.

Die kantonalen Parlamente bleiben selbstverständlich in jenen Bereichen autonom, in denen die kantonalen Behörden ausserhalb dieser Vorlage für die innere Sicherheit ihres Gebietes tätig sind.

#### *Art. 70*            Kantonale Aufsicht

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

##### *Aufsicht durch den Bund*

Die Oberaufsicht über den materiell richtigen Vollzug dieses Gesetzes und somit auch über die Tätigkeit der kantonalen Vollzugsbehörden obliegt der Geschäftsprüfungsdelegation der Eidgenössischen Räte. Die interne Aufsichtsinstanz des VBS kann zudem Kontrollen bei den kantonalen Vollzugsbehörden durchführen (Art. 66 Abs. 3).

##### *Aufsicht durch die Kantone*

Die Aufsicht der Kantone besteht im Wesentlichen 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, und
- 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 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 *Bundslösung* hätte den Vorteil einer einheitlichen Regelung der Aufsicht über die kantonalen Vollzugsbehörden. 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 seiner Bevölkerung zuständig sind (Art. 57 Abs. 1 BV). Die Einführung einer reinen Bundslösung 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 einer einheitlichen Regelung für alle Kantone. 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 Oberaufsicht über die Tätigkeit der kantonalen Vollzugsbehörden zufallen würde, unterschiedliche Praxen 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. Ferner würden sich schwierige Abgrenzungsfragen bezüglich der Aufsicht über die Auftragserteilung des Bundesorgans ergeben. Der NDB würde wohl in Teilen auch den kantonalen Aufsichtsorganen gegenüber rechenschaftspflichtig, was wiederum systemwidrig wäre. Auch die kantonale Lösung vermag deshalb insgesamt nicht zu überzeugen.

Der Bundesrat ist aus diesen Gründen der Auffassung, dass an der bisherigen geteilten Aufsicht von Bund und Kantonen festzuhalten ist.

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* soll klargestellt werden, dass die parlamentarische Oberaufsicht über den Vollzug dieses Gesetzes bei der Geschäftsprüfungsdelegation der Eidgenössischen Räte liegt und nicht gleichzeitig (ganz oder teilweise) bei einem kantonalen Gremium.

### 3. Abschnitt: Rechtsschutz

#### Art. 71 Rechtsschutz

Das NDG definiert 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. Sie fallen damit klarerweise nicht unter die Ausnahmeregelung von Artikel 83 Buchstabe a des Bundesgesetz vom 17. Juni 2005<sup>28</sup> über das Bundesgericht, der Entscheide auf dem Gebiet der inneren oder äusseren Sicherheit des Landes von der Beschwerde in öffentlich-rechtlichen Angelegenheiten ausnimmt.

*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 4* den Beginn der Beschwerdefrist auf den Erhalt der Mitteilung fest.

### 7. Kapitel: Schlussbestimmungen

#### Art. 72 Ausführungsbestimmungen

Gemäss Artikel 7 des Regierungs- und Verwaltungsorganisationsgesetzes erlässt der Bundesrat die Verordnungen, soweit er dazu durch Verfassung oder Gesetz ermächtigt ist (vgl. auch Art. 182 Abs. 1 BV). Artikel 72 beauftragt den Bundesrat zusätzlich zu den besonderen Delegationen im Gesetz, allgemeine Vollzugsvorschriften zu erlassen.

#### Art. 73 Vollzug durch 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 Bundesrats zur Erfüllung des Postulates Malama vom 2. März 2012<sup>29</sup>). 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

<sup>28</sup> SR 173.110

<sup>29</sup> BBl 2012 4459

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 „Malama-Bericht“ des Bundesrates 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 Polizeihochheit 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 obliegt. 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 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 auf Grund 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.

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 Entschädigungen 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 Entschädigung, welche die Aufwände der Kantone nur zu einem Teil deckt, festhalten und sie nicht als mit dem allgemeinen Finanzausgleich zwischen Bund und Kantonen als abgegolten betrachten.

## Änderung bisherigen Rechts

### I Aufhebung von Erlassen

Der vorliegende Entwurf übernimmt die polizeirechtlichen Bestimmungen des BWIS nicht (Schutz von Personen und Gebäuden, Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen, Beschlagnahmung von Gewaltpropaganda). Die Bestimmungen mit polizeirechtlichem Charakter sind Gegenstand des künftigen Polizeiaufgabengesetzes, welches sich ebenfalls in Erarbeitung befindet.

Für den Fall, dass das Nachrichtendienstgesetz vor dem Polizeiaufgabengesetz in Kraft treten kann, würde der Bundesrat über den Weg der teilweisen In- bzw. Ausserkraftsetzung dafür sorgen, dass keine rechtlichen Lücken entstehen.

Analoges gilt für den Bereich Personensicherheitsprüfungen (PSP), wo ebenfalls eine neue Vorlage in Vorbereitung ist (Informationssicherheitsgesetz), die diesen Bereich des BWIS übernehmen wird. Die PSP-Bestimmungen figurieren deshalb nicht mehr in dieser Vorlage.

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

### II Änderung von Erlassen

#### 1. Bundesgesetz vom 20. Juni 2003<sup>30</sup> über das Informationssystem für den Ausländer- und den Asylbereich

*Art. 9 Abs. 1 Bst. c und l (neu)*

In Artikel 9 Absatz 1 Buchstabe c BGIAA (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 Fernhaltungsmassnahmen 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. Wir schlagen deshalb vor, die Voraussetzungen für den Online-Zugriff entsprechend den gesetzlichen Aufgaben des NDB zu entsprechend 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<sup>31</sup> und im Asylgesetz vom 26. Juni 1998<sup>32</sup> in zahlreichen Bestimmungen enthalten, weshalb hier der Gesetzestext auf einzelne Erwähnungen verzichtet.

<sup>30</sup> SR 142.51

<sup>31</sup> SR 142.20

<sup>32</sup> SR 142.31

## **2. Archivierungsgesetz vom 26. Juni 1998<sup>33</sup>**

*Art. 14 Abs. 2 Bst. a<sup>bis</sup> (neu)*

Diese Ergänzung soll eine bisherige Lücke im Archivrecht schliessen. Dritte haben zwar teilweise die Möglichkeit zur Einsichtnahme in archivierte Akten zur inneren und äusseren Sicherheit, nicht aber die abliefernde Amtsstelle, hier der Nachrichtendienst, wenn es um eine erneute Einschätzung von Bedrohungen geht, für welche die archivierten Akten Aufschluss geben können. Das BGA soll deshalb um diesen Aspekt der Wahrung der inneren und äusseren Sicherheit ergänzt werden.

## **3. Öffentlichkeitsgesetz vom 17. Dezember 2004<sup>34</sup>**

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 ungenügend mit dem Transparenzgedanken des BGÖ vereinbar ist.

Die bisherigen Zugangsgesuche betrafen jeweils auch Dokumente und Dossiers über die Beschaffung von Informationen durch den NDB oder über Aktionen, die der NDB (oder seine Vorgänger) durchgeführt hatten. Vereinzelt wurde auch Einsicht in andere Unterlagen, z.B. über den Verkehr mit ausländischen Partnerdiensten, verlangt. Mit Rücksicht auf die beteiligten Personen oder Partnerdienste musste der NDB die Einsicht in Beschaffungs- und Partnerdienst dossiers jeweils ablehnen. Die Gesuche lösten zum Teil einen beträchtlichen Aufwand aus, da die gewünschten Dokumente umfassend zusammengestellt und bewertet werden mussten. Teilweise waren diese Dokumente sehr umfangreich und umfassten mehrere 100 Seiten.

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 BGÖ durchaus möglich ist, schlägt der Bundesrat nur eine sachliche Ausnahme für die Unterlagen über die nachrichtendienstliche Informationsbeschaffung vor.

## **4. Verwaltungsgerichtsgesetz vom 17. Juni 2005<sup>35</sup>**

Art. 23 Abs. 2 und Art. 36b Genehmigung von Beschaffungsmassnahmen des Nachrichtendienstes

In Art. 23 Abs. 2 Bst. b wird die Zuständigkeit der Präsidentin oder des Präsidenten der zuständigen Abteilung des Bundesverwaltungsgerichts für das Genehmigungsverfahren betreffend die bewilligungspflichtigen Beschaffungsmassnahmen und betreffend die Kabelaufklärung eingeführt.

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

<sup>33</sup> SR 152.1

<sup>34</sup> SR 152.3

<sup>35</sup> SR 173.32

#### *Art. 33 Bst. b Ziff. 4*

Die Beschwerde gegen Verfügungen des Bundesrates über Tätigkeitsverbote (Art. 31) muss explizit vorgesehen werden, da sie bisher in der abschliessenden Aufzählung nach Artikel 33 Buchstabe b VGG nicht enthalten ist.

### **5. Zivilgesetzbuch<sup>36</sup>**

#### *Art. 43a Abs. 4 Ziff. 5 (neu)*

Mit der Ergänzung in Artikel 43a Absatz 4 ZGB soll dem NDB der Zugriff auf das System Infostar (Zivilstandsregister) zum Zwecke der Identifizierung von Personen, sowie ihres gegenwärtigen und allenfalls früheren Aufenthalts ermöglicht werden. Da das ZGB bei den anderen zugriffsberechtigten Stellen keine Zweckbindung erwähnt, erfolgt auch bezüglich des NDB keine. 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.

### **6. Strafgesetzbuch<sup>37</sup>**

#### *Art. 317<sup>bis</sup> Abs. 1 und 2*

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

#### *Art. 365 Abs. 2 Bst. r (neu), s (neu), t (neu) und u (neu)*

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 im Rahmen der bestehenden Aufgaben nach Artikel 365 Absatz 2. Diese decken jedoch das Aufgabenspektrum des NDB teilweise nur rudimentär ab. Es ist deshalb gerechtfertigt, bei der neuen Gesetzgebung über den Nachrichtendienst diese Aufzählung zu komplettieren. Neu ist insbesondere die Erwähnung der Überprüfung der Unbedenklichkeit von Personen regeln, die an ausländischen klassifizierten Projekten mitarbeiten oder Zugang zu klassifizierten Informationen, Materialien oder Anlagen des Auslands erhalten sollen (vgl. Art. 10 Absatz 1 Buchstabe d).

#### *Art. 367 Abs. 2 Bst. m (neu) und Abs. 4*

Der NDB benötigt für die Erfüllung seiner gesetzlichen Aufgaben nicht nur Kenntnis von erfolgten Verurteilungen, sondern auch von allfällig hängigen Strafverfahren. Dies dient zum einen nicht nur der Verhinderung von Überschneidungen nachrichtendienstlicher Aktivitäten mit solchen der Strafverfolgungsorgane, sondern

<sup>36</sup> SR 210

<sup>37</sup> SR 311.0

auch der korrekten Auskunftserteilung bei Unbedenklichkeitsabklärungen nach Artikel 10 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.

## **7. Bundesgesetz vom 13. Juni 2008<sup>38</sup> über die polizeilichen Informationssysteme des Bundes**

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 zur Ausschreibung zur Aufenthaltsfeststellung nach Artikel 14 NDG. Zugriff auf Daten werden nicht sämtliche Mitarbeitenden des NDB haben, sondern nur jene, welche ihn für die Erfüllung der gesetzlich vorgesehenen Aufgaben benötigen. Der Bundesrat wird wie üblich in den Ausführungsverordnungen den Kreis der zugriffsberechtigten Mitarbeitenden des NDB und den Umfang ihrer Zugriffe näher regeln.

## **8. Militärgesetz vom 3. Februar 1995<sup>39</sup>**

*Art. 99 Abs. 1<sup>bis</sup>, 1<sup>quater</sup> (neu) und 3<sup>bis</sup> (neu)*

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

Absatz 1<sup>quater</sup> stellt dem Nachrichtendienst der Armee dasselbe Mittel für die Beobachtung aus der Luft zu Verfügung wie dem NDB (Art. 12) und nimmt auch dessen Vorkehren zum Schutz der Privatsphäre auf.

Absatz 3<sup>bis</sup> entspricht der entsprechenden Bestimmung von Artikel 60 Absatz 2 NDG.

## **9. Bundesgesetz vom 3. Oktober 2008<sup>40</sup> über die militärischen Informationssysteme**

*Art. 16 Abs. 1 Bst. h (neu)*

Der Online-Zugriff durch den NDB auf die PISA-Datenbank ist neu vorgesehen, damit der NDB mögliche Bedrohungen für die Sicherheit der Armee durch Personen feststellen kann, die beispielsweise gewaltextremistischen 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

<sup>38</sup> SR 361

<sup>39</sup> SR 510.10

<sup>40</sup> SR 510.91

Armee in der Handhabung von Waffen und Sprengstoffen und der Anwendung von Kampfverfahren ausgebildet werden.

## **10. Kernenergiegesetz vom 21. März 2003<sup>41</sup>**

*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 zum Vollzug des KEG sowie für die Deliktsverhütung und die Strafverfolgung. In der Praxis hat sich gezeigt, dass es notwendig ist, den Tätigkeitsbereich der Zentralstelle auf den Bereich des Strahlenschutzgesetzes auszudehnen, der mit demjenigen des KEG 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 beispielsweise bei der Aufnahme der Bearbeitung eines Falles von Atomschmuggel noch nicht beurteilt werden können.

## **11. Strassenverkehrsgesetz vom 19. Dezember 1958<sup>42</sup>**

*Art. 104c Abs. 5 Bst. c (neu)*

Mittels der Anpassung von Artikel 104c 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.

## **12. Bundesgesetz vom 6. Oktober 2000<sup>43</sup> betreffend die Überwachung des Post- und Fernmeldeverkehrs**

*Art. 1 Abs. 1 Bst. d*

Der NDB kann neu Überwachungen des Post- und Fernmeldeverkehrs anordnen (Art. 22 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 Art. 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

<sup>41</sup> SR 732.1

<sup>42</sup> SR 741.01

<sup>43</sup> SR 780.1

Korrelat zur Befugnis des NDB nach Artikel 22 Absatz 1 Buchstaben a-d NDG, den Post- und Fernmeldeverkehr einer Person überwachen zu lassen.

*Art. 14 Abs. 2<sup>bis</sup>*

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

### **13. Fernmeldegesetz vom 30. April 1997<sup>44</sup>**

*Art. 34 Abs. 1<sup>ter</sup> und 1<sup>quater</sup> (neu)*

Neu wird in diesem Absatz auch der NDB erwähnt. Damit wird im FMG das erforderliche, formellgesetzliche Pendant zu Artikel 5 Absatz 1 Buchstabe d NDG geschaffen. Gleichzeitig wird die Koordination zwischen den beiden Gesetzen hergestellt.

### **Zusammenfassender Hinweis zu den Ziffern 14ff.:**

Bei den nachfolgenden Erlassen 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 Auskunftgabe „im Einzelfall auf schriftlich begründetes Gesuch hin“ gestrichen. Dieser Verweis hat sich als unnötig erwiesen, weil jede Auskunftgabe an den NDB bereits in der jeweils vorangestellten Bestimmung mit enthalten ist. Es erfolgt somit lediglich eine Korrektur eines gesetzgeberischen Versehens und keine Änderung der Rechtslage.

### **14. Bundesgesetz vom 20. Dezember 1946<sup>45</sup> über die Alters- und Hinterlassenenversicherung**

*Art. 50a Abs. 1 Bst. d<sup>bis</sup> und e Ziffer 7*

### **15. Bundesgesetz vom 19. Juni 1959<sup>46</sup> über die Invalidenversicherung**

*Art. 66a Abs. 1 Bst. c*

### **16. Bundesgesetz vom 25. Juni 1982<sup>47</sup> über die berufliche Alters-, Hinterlassenen und Invalidenvorsorge**

<sup>44</sup> SR 784.10

<sup>45</sup> SR 831.10

<sup>46</sup> SR 831.20

*Art. 86a Abs. 1 Bst. g sowie Abs. 2 Bst. g*

### **17. Bundesgesetz vom 18. März 1994<sup>48</sup> über die Krankenversicherung**

*Art. 84a Abs. 1 Bst. g<sup>bis</sup> und h Ziff. 6*

### **18. Bundesgesetz vom 20. März 1981<sup>49</sup> über die Unfallversicherung**

*Art. 97 Abs. 1 Bst. h<sup>bis</sup> und i Ziff. 6*

### **19. Bundesgesetz vom 19. Juni 1992<sup>50</sup> über die Militärversicherung**

*Art. 1a Abs. 1 Bst. q*

Diese Bestimmung bildet das Pendant zu Artikel 32 Absatz 6 NDG, wonach die im Ausland eingesetzten Mitarbeiterinnen und Mitarbeiter des NDB der Militärversicherung unterstellt sind. Diese Bestimmung soll auch im MVG als Quellerlass verankert werden.

*Art. 95a Abs. 1 Bst. h<sup>bis</sup> und i Ziff. 8*

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

### **20. Arbeitslosenversicherungsgesetz vom 25. Juni 1982<sup>51</sup>**

*Art. 97a Abs. 1 Bst. e<sup>bis</sup> und f Ziff. 8*

<sup>47</sup> SR 831.40

<sup>48</sup> SR 832.10

<sup>49</sup> SR 832.20

<sup>50</sup> SR 833.1

<sup>51</sup> SR 837.0

## Informationsbeschaffungsmassnahmen gemäss Entwurf zum Nachrichtendienstgesetz

Beschaffung im Inland		Beschaffung im Ausland	
Beschaffungszweck	Genehmigungsfreie Massnahmen nach Art. 11ff.	Genehmigungspflichtige Massnahmen nach Art. 22ff.	
1. Art. 4 Abs. 1 Bst. a Ziff. 1-5: → Terrorismus → Verbotener Nachrichtendienst → Proliferation → Angriffe auf kritische Infrastrukturen	Anwendbar	Anwendbar	1. <i>Verdeckte Beschaffungsmassnahmen</i> (Art. 32) Voraussetzung: Beschaffung sicherheitspolitisch bedeutsamer Informationen über das Ausland nach Art. 4 Abs. 1 Bst. b.
2. Art. 4 Abs. 1 Bst. a Ziff. 6: → Gewalttätiger Extremismus	Anwendbar	Nicht anwendbar	2. <i>Funkaufklärung</i> (Art. 33) Voraussetzung: Beschaffung sicherheitspolitisch bedeutsame Informationen über das Ausland.  Informationen über Vorgänge im Inland dürfen nur weitergeleitet werden, wenn sie auf eine konkrete Gefährdung der inneren Sicherheit hinweisen (Art. 33 Abs. 5).  3. <i>Kabelaufklärung</i> (Art. 34ff.) Zur Beschaffung von Informationen über sicherheitspolitische Vorgänge im Ausland sowie zur Wahrung wesentlicher Landesin-

			teressen (Art. 62) können Signale aus leitungsgebundenen Netzen erfasst werden.
3. Informationsbeschaffung im Inland über Vorgänge im Ausland (Art. 32 Abs. 2)	Anwendbar	Anwendbar. Bewilligung grundsätzlich analog Beschaffung Inland. Ausnahme: Eindringen in Computersysteme, wenn sich die betroffenen Systeme im Ausland befinden (Art. 32 Abs. 2).	
Wahrung weiterer wesentlicher Landesinteressen			
Der Bundesrat kann den NDB zur Wahrung weiterer wesentlicher Landesinteressen im Sinne von Artikel 1 Absatz 3 mit Massnahmen nach dem vorliegenden Gesetz beauftragen (Art. 62).			