

Bundesversammlung

Assemblée fédérale

Assemblea federale

Assamblea federala



Geschäftsprüfungsdelegation  
CH-3003 Bern

[www.parlament.ch](http://www.parlament.ch)  
[gpk.cdg@parl.admin.ch](mailto:gpk.cdg@parl.admin.ch)

## Einschreiben

An die  
Sicherheitspolitische Kommission  
des Nationalrats  
Parlamentsgebäude  
3003 Bern

22. April 2014

### Mitbericht der Geschäftsprüfungsdelegation zum NDG (14.022)

Sehr geehrter Herr Präsident  
Sehr geehrte Damen und Herren Nationalräte

Die GPDel nimmt zusammen mit der FinDel die Oberaufsicht des Parlaments über den Bereich des Staatschutzes und des Nachrichtendienstes wahr. Aufgrund ihrer Tätigkeit hat die GPDel verschiedentlich Rechtsetzungsbedarf in diesen Bereichen festgestellt und dazu auch Empfehlungen an den Bundesrat gerichtet.

Die GPDel hat bisher das Mittel des Mitberichts insbesondere benutzt, um im Bedarfsfall den Empfehlungen aus ihren Inspektionen Nachdruck zu verleihen. So äusserte sich die GPDel zu allen nachrichtendienstlichen Gesetzesvorlagen der letzten Jahre, beispielsweise zur BWIS-II-Revision vom 15. Juni 2007 (07.057) und zur Zusatzbotschaft dazu vom 27. Oktober 2010 sowie zur ZNDG-Revision (13.064) vom 14. August 2013.

Nach Einschätzung der GPDel stellt das NDG das bisher umfassendste Reformprojekt für den Staatschutz und den Nachrichtendienst in der Schweiz dar. Seine Ziele sind breiter als diejenigen des ursprünglichen BWIS (Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit von 1997) und höher gesteckt als diejenigen der gescheiterten BWIS-II-Vorlage von 2007. Die Vorlage kann überdies für die zukünftige Arbeit der GPDel und ihrer institutionelle Rolle grundlegende Auswirkungen haben.

Aus diesen Gründen beschränkt sich der Mitbericht der GPDel (vgl. Anhang) nicht auf einzelne Aspekte der Vorlage, sondern versucht vornehmlich aus der Perspektive der Aufsichts- und Kontrollverfahren, Verbesserungsvorschläge über die ganze Vorlage hinweg einzubringen. Im Anhang finden Sie Anträge und Empfehlungen zu rund 30 Punkten, welche aus Sicht der Delegation die besondere Aufmerksamkeit Ihrer Kommission verdient.

In ihrer Funktion als Oberaufsicht ist es der GPDel ein besonderes Anliegen, dass das NDG eine lückenlose Kontrolle seitens der Exekutive sicherstellt. Es kann nicht die Aufgabe der GPDel sein, Lücken in der Führung und der Aufsicht seitens des Bundesrats und des zuständigen Departements zu kompensieren. Dieses Prinzip ist umso wichtiger je umfassender die Kompetenzen und Aufgaben des Nachrichtendienstes werden.



Die technische Entwicklung hat zur Folge, dass sich ein wachsender Anteil des menschlichen Lebens im digitalen Raum abspielt oder dort zumindest abgebildet wird. Dies trifft auch für die Aktivitäten zu, welche die innere und äussere Sicherheit der Schweiz bedrohen können. Für die GPDel ist es deshalb unbestritten, dass die Möglichkeiten des Nachrichtendienstes dieser Entwicklung angepasst werden müssen, wie dies auch für die Strafverfolgung mit der hängigen BÜPF-Revision angestrebt wird.

Die GPDel befürwortet eine Gesamtkodifikation der Aufgaben und Kompetenzen des NDB in einem neuen Gesetz. Gleichzeitig ist sie sich auch der Herausforderung bewusst, die allgemeingültigen Anforderungen an den Schutz der Persönlichkeit und an eine funktionierende Aufsicht mit den unterschiedlichen Umständen, die für die nachrichtendienstliche Tätigkeit im In- und Ausland gelten, zu vereinbaren.

Aufgrund ihrer bisherigen Erfahrungen mit dem NDB beurteilt die GPDel diese Vorlage aber auch aus der Sicht ihrer späteren Umsetzung, welche sie dann in ihrer Eigenschaft als Oberaufsicht zu begleiten hat. Es ist deshalb der GPDel ein zentrales Anliegen, dass die neuen Aufgaben und Kompetenzen und die dafür vorgesehenen zusätzlichen Personalressourcen im richtigen Verhältnis zueinander stehen (vgl. Empfehlung 1 der GPDel-Inspektion zur Informatiksicherheit im NDB).

Wir versichern Sie, sehr geehrter Herr Präsident, sehr geehrte Damen und Herren Nationalräte, unserer vorzüglichen Hochachtung.

#### **GESCHÄFTSPRÜFUNGSDELEGATION**

Der Präsident

Die Sekretärin

Paul Niederberger  
Ständerat

Beatrice Meli Andres

Anhang: Mitbericht der GPDel vom 22. April 2014

Kopie an: FinDel



22. April 2014

## Mitbericht der GPDel zum E-NDG (14.022), Anhang

|     |                                                                                                       |    |
|-----|-------------------------------------------------------------------------------------------------------|----|
| 1.  | Oberaufsicht auf Stufe Bund und in den Kantonen (Art. 77 und 78).....                                 | 3  |
| 2.  | Dienstaufsicht in den Kantonen (Art. 76 und 78).....                                                  | 4  |
| 3.  | Informationsrechte der GPDel (Art. 76 und 70).....                                                    | 6  |
| 4.  | Führung durch den Bundesrat (Art. 69).....                                                            | 7  |
| 5.  | Aufsicht und Kontrolle durch den Bundesrat (Art. 76).....                                             | 8  |
| 6.  | Konsultation des SiA (Art. 29) .....                                                                  | 9  |
| 7.  | Aufsicht durch das VBS (Art. 74).....                                                                 | 10 |
| 8.  | Aufgaben des NDB (Art. 3, 6, 16, 19, 26, 37 und 70) .....                                             | 11 |
| 9.  | Auskunftspflichten von Behörden (Art. 19 und 20).....                                                 | 12 |
| 10. | Meldungen und Auskünfte von Dritten (Art. 22) .....                                                   | 14 |
| 11. | Anhaltung von Dritten (Art. 23).....                                                                  | 15 |
| 12. | Besondere Auskunftspflicht Privater (Art. 24) .....                                                   | 16 |
| 13. | Verfahren für genehmigungspflichtige Beschaffungsmassnahmen (Art. 28 und 31a).....                    | 17 |
| 14. | Oberaufsicht gegenüber dem BVGer (Art. 28) .....                                                      | 19 |
| 15. | Koordination zwischen dem E-NDG und der Revision des BÜPF .....                                       | 20 |
| 16. | Eindringen in ein Computersystem zur Informationsbeschaffung (Art. 25 und 36).....                    | 21 |
| 17. | Sabotage von Computersystemen im Inland (Art. 25 und 28) .....                                        | 22 |
| 18. | Sabotage von Computersystemen im Ausland (Art. 36) .....                                              | 24 |
| 19. | Kooperation mit Partnerdiensten in der Beschaffung (Art. 33 Abs. 1) .....                             | 25 |
| 20. | Kooperation mit Privaten in der Beschaffung (Abs. 33 Abs. 2) .....                                    | 25 |
| 21. | Quellenschutz gegenüber den Strafverfolgungsbehörden (Art. 34 Abs. 2 und 4) .....                     | 26 |
| 22. | Funkaufklärung und ihre Kontrollinstanz (Art. 37 und Art. 75) .....                                   | 27 |
| 23. | Kabelaufklärung (Art. 38 – 42).....                                                                   | 28 |
| 24. | Datenbanken und Qualitätskontrollen (Art. 43 – 56) .....                                              | 29 |
| 25. | Ungeklärte Kosten/Nutzen-Frage bei Quattro P / P4 (Art. 54) .....                                     | 31 |
| 26. | Qualitätskontrollen bei Informationen aus beschaffungspflichtigen Massnahmen<br>(Art. 46 und 57)..... | 32 |



|     |                                                           |    |
|-----|-----------------------------------------------------------|----|
| 27. | Weitergabe von Personendaten ans Ausland (Art. 60).....   | 33 |
| 28. | Auskunftsrecht (Art. 63).....                             | 34 |
| 29. | Archivierung (Art. 67).....                               | 35 |
| 30. | Beobachtungsliste (Art. 71) .....                         | 36 |
| 31. | Personelle Auswirkungen (Ziff. 3.1.2 der Botschaft) ..... | 37 |





## Anhang zum Mitbericht der GPDel zum E-NDG (14.022)

### 1. Oberaufsicht auf Stufe Bund und in den Kantonen (Art. 77 und 78)

#### **Problematik**

In den Kantonen sollen die bisherigen rechtlichen Möglichkeiten für eine Oberaufsicht durch die kantonalen Parlamente erhalten bleiben.

#### **Anträge der GPDel**

##### Art. 77 Parlamentarische Oberaufsicht

1 Die parlamentarische Oberaufsicht über die Tätigkeit des NDB und der im Auftrag des NDB Bundes handelnden kantonalen Vollzugsorgane zum Vollzug dieses Gesetzes obliegt in ihren jeweiligen Zuständigkeitsbereichen ~~ausschliesslich~~ der Geschäftsprüfungsdelegation und der Finanzdelegation nach Massgabe des Parlamentsgesetzes vom 13. Dezember 2002.

2 ~~Kantonale parlamentarische Aufsichtsorgane können den Vollzug nach Artikel 81 Absatz 1 NDG überprüfen.~~

##### Art. 78 Kantonale Aufsicht

~~2 Kantonale parlamentarische Aufsichtsorgane können den selbstständigen Vollzug nach Artikel 81 Absatz 1 beaufsichtigen. Für die Aufsicht über den Vollzug von Aufträgen des NDB nach Artikel 9 Absatz 2 oder die Beschaffung von Informationen über Organisationen und Gruppierungen der Beobachtungsliste nach Artikel 71 gilt Artikel 77.~~

[Vorschlag für Neuformulierung dieses Absatzes in Ziff. 2 betr. Dienstaufsicht in den Kantonen, S.4].

#### **Begründung**

Laut Art. 77 E-NDG soll die Oberaufsicht über die Tätigkeit der im Auftrag des NDB handelnden kantonalen Vollzugsorgane ausschliesslich in die Kompetenz der GPDel und FinDel fallen.

Demgegenüber erlaubt Art. 78 Abs. 2 E-NDG im Prinzip auch eine Oberaufsicht über den Vollzug des E-NDG in den Kantonen.

Der zweite Satz von Art. 78 Abs. 2 E-NDG schränkt jedoch die Kompetenz der kantonalen Oberaufsicht wieder grundlegend ein, indem er jegliche kantonale Tätigkeit davon ausnimmt, wenn sie dem Vollzug von Aufträgen des NDB oder der Informationsbearbeitung zu Organisationen der Beobachtungsliste dient. Nach den Erläuterungen soll sich die parlamentarische Oberaufsicht in den Kantonen ausschliesslich auf „die Tätigkeiten der kantonalen Vollzugsbehörden beschränken, die diese selbstständig in direkter Anwendung des NDG vornehmen, ohne dass sie im Einzelfall hierzu einen ausdrücklichen Auftrag des NDB erhalten haben“ (Botschaft NDG vom 19.2.2014, S. 102).

Noch am 8. März 2013 führte der Bundesrat allerdings in den Erläuterungen zur Vernehmlassung aus: „Die kantonalen Sicherheitsorgane werden immer im direkten Vollzug des Gesetzes zu Handen der Bundesorgane tätig und nicht im originären Vollzugsinteresse der Kantone“ (Bericht zum Vorentwurf NDG vom 8.3.2014, S. 71). Eine Oberaufsicht durch die kantonalen Parlamente war im damaligen Entwurf aber auch nicht vorgesehen.

Wie die GPDel anlässlich ihrer Besuche bei den kantonalen Staatsschutzorganen feststellen konnte, ist gerade die Beobachtungsliste des Bundesrats ein wichtiger Leitfaden für die



Priorisierung der Staatsschutzfähigkeit in den Kantonen. Die GPDel stellte auch fest, dass die Kantone so gut wie keine Staatsschutzaufgaben wahrnehmen, die nicht in einem Zusammenhang mit der Tätigkeit des NDB stehen. In der heutigen Welt, in welcher die Bedrohung durch eine Vernetzung auf nationaler und internationaler Ebene geprägt ist, wäre ein anderes Vorgehen auch nicht zweckmässig.

Der Bundesrat macht in der aktuellen Vorlage geltend, dass das bisherige Recht (BWIS und ParlG) die parlamentarische Oberaufsicht auf Stufe Bund und Kanton ausschliesslich der GPDel zugewiesen habe (Botschaft NDG, S. 100).

Demgegenüber war der Bundesrat in seinem Bericht zur Erfüllung des Postulats Malama (10.3045) vom 2. März 2012 noch der Meinung, dass sich das Bundesrecht über die kantonale parlamentarische Kontrolle ausschweige und eine parlamentarische Oberaufsicht somit auf Kantonsebene nicht ausschliesse. Dies ergäbe sich auch aus dem Grundsatz, dass die kantonale Organisationsautonomie (Art. 47 Abs. 2 BV) auch bei der Umsetzung von Bundesrecht so weit wie möglich zu wahren sei. (Bericht zu Po. Malama vom 2.3.2012, BBl 2012 4501/4502).

In der Vernehmlassung verlangten immerhin zwölf Kantonsparlamente in einem Schreiben der Interkantonalen Legislativkonferenz (ILK) vom 28. Juni 2013, dass auch unter dem neuen Gesetz die kantonale Dienstaufsicht und die kantonale Oberaufsicht sowohl de jure als auch de facto uneingeschränkt möglich blieben. Ebenso sollte der Grundsatz gelten, dass die kantonale Oberaufsicht gleich weit geht wie die kantonale Dienstaufsicht (Akzessorietätsprinzip).

Die GPDel ging bisher ebenfalls davon aus, dass die kantonalen GPKs eine Rolle bei der Oberaufsicht über die kantonalen Staatsschutzorgane haben können (vgl. Ziff. 2). Auf dieser Grundlage tauschte sich die GPDel in der Vergangenheit mit kantonalen GPKs aus (LU, BL).

Die GPDel teilt auch nicht die Befürchtung des Bundesrats, dass eine Zuständigkeit sowohl der GPDel als auch der kantonalen GPK Lücken in der Oberaufsicht verursachen würde (Botschaft NDG, S. 98, 100, 102). Sind die Parlamente einzelner Kantone bereit, Verantwortung zu übernehmen, entstehen dadurch keine Aufsichtslücken, sondern vielmehr Chancen für Synergien und für eine koordinierte Zusammenarbeit.

Bereits rein praktisch wäre es unmöglich für die GPDel, die kantonalen Staatsschutzstellen ähnlich systematisch zu kontrollieren, wie sie es mit dem NDB, dem Militärischen Nachrichtendienst (MND) und dem Zentrum für elektronische Operationen (ZEO) macht. Es gilt auch zu bedenken, dass die neuen Aufgabengebiete und die zusätzlichen Kompetenzen für die Informationsbeschaffung des NDB der GPDel zusätzliche Arbeit verursachen würden.

Soweit es der GPDel aus ihrer institutionalisierten Zusammenarbeit mit der FinDel bekannt ist, hat sich diese noch nie mit den kantonalen Staatsschutzorganen befasst. Falls die FinDel hier neue Aufgaben erhalten sollte, müsste auch geklärt werden, inwiefern sie dafür auf die Unterstützung der Eidg. Finanzkontrolle (EFK) zählen könnte.

## **2. Dienstaufsicht in den Kantonen (Art. 76 und 78)**

### ***Problematik***

Die Aufsicht durch die Exekutive der Kantone, für die im Jahr 2010 auf Initiative der KKJPD eine Lösung gefunden wurde, die sich bewährt hat, soll im E-NDG übernommen werden. Die konkrete Ausgestaltung soll nicht allein dem Bundesrat überlassen werden, sondern mit Rücksicht auf die Autonomie der Kantone in den Grundzügen ins Gesetz geschrieben werden.



## **Anträge der GPDeI**

### **Art. 78 Kantonale Aufsicht**

1 Angehörige der kantonalen Vollzugsbehörden, die von den Kantonen mit Aufgaben nach diesem Gesetz betraut sind, unterstehen dem kantonalen Dienstrecht und der kantonalen Dienstaufsicht ihrer Vorgesetzten. [unverändert]

2 (neu) *Die Dienstaufsicht in den Kantonen obliegt denjenigen Stellen, die dem jeweiligen kantonalen Vollzugsorgan vorgesetzt sind. Diese können zur Unterstützung der Dienstaufsicht ein vom kantonalen Vollzugsorgan getrenntes Kontrollorgan einsetzen, das den vorgesetzten Stellen verantwortlich ist. [wie Art. 35 Abs. 1 V-NDB]*

3 (neu) *Für ihre Kontrollen erhält die kantonale Aufsicht eine Liste der vom NDB erteilten Aufträge sowie die Beobachtungsliste nach Artikel 71. [wie Art. 35 Abs. 3 Bst. c V-NDB]*

4 (neu) *Die kantonale Dienstaufsicht kann Einsicht nehmen in die Daten, die der Kanton im Auftrag des Bundes bearbeitet. Die Einsicht kann verweigert werden, wenn wesentliche Sicherheitsinteressen dies erfordern. [wie Art. 35a Abs. 1 und 4 V-NDB]*

5 (neu) *Der Bundesrat regelt das Einsichtsverfahren. Bei Streitigkeiten steht die Klage ans Bundesgericht nach Artikel 120 Absatz 1 Buchstagen b Bundesgerichtsgesetz offen.*

6 (neu) *Der Bundesrat regelt die Unterstützung der kantonalen Dienstaufsicht durch Stellen des Bundes. [wie Art. 35a Abs. 4 V-NDB]*

### **Art. 76 Aufsicht und Kontrolle durch den Bundesrat**

3 Er regelt:

b. die Mindestanforderungen an die Kontrolle in den Kantonen und die Zuständigkeiten von Aufsichtsorganen des Bundes ~~und der Kantone~~.

## **Begründung**

Die Informationsrechte der kantonalen Dienstaufsicht hatten die GPDeI bereits anlässlich ihrer ISIS-Inspektion beschäftigt.

Wie die GPDeI in ihrem Bericht ausführte, entwickelte als Folge der „Basler Fichen-Affäre“ im Frühjahr 2010 die Konferenz der Kantonalen Justiz- und Polizeidirektoren (KKJPD) einen Lösungsvorschlag. Dieser sah vor, dass die kantonale Aufsicht die konkreten Aufträge des Bundes an das kantonale Staatsschutzorgan kennt und dessen Arbeit anhand dieser Vorgaben überprüfen kann. Falls der NDB Einsicht in die Staatsschutzdaten, die im Kanton aufgrund der Aufträge des Bundes bearbeitet werden, ablehnen würde, sollte der Kanton an das VBS gelangen können. Nach einem Entscheid des Vorstehers VBS würde den Kantonen zudem der Weg der Klage ans BGer nach Art. 120 Abs. 1 Bst. b BGG (Bundesgerichtsgesetz) offen stehen (vgl. ISIS-Bericht der GPDeI vom 21.6.2010, BBl 2010 7717). Mit der Revision der V-NDB vom 18. August 2010 übernahm der Bundesrat im Wesentlichen den Vorschlag der KKJPD (Art. 35ff V-NDB, Verordnung über den NDB).

Im Hinblick auf die Zusatzbotschaft zur BWIS-II-Revision liess die GPDeI von Prof. Biaggini die Notwendigkeit einer Regelung der kantonalen Aufsicht im Gesetz abklären. In ihrem Mitbericht an die RK-S vom 24. März 2011 ging die GPDeI in der Folge davon aus, dass eine funktionierende Aufsicht durch die Kantone gestützt auf die existierenden rechtlichen Grundlagen prinzipiell möglich sei. Deshalb erachtete die GPDeI einen Antrag zu einer weitergehenden Regelung der kantonalen Aufsichtskompetenzen im Gesetz nicht für nötig.



Die Delegation wollte jedoch das Thema weiter verfolgen, um rechtzeitig einen gesetzgeberischen Handlungsbedarf erkennen zu können.

Die heutigen Art. 35ff V-NDB regelt in materieller Hinsicht die Aufgaben der kantonalen Dienstaufsicht zweckmässig. Es ist aber fraglich, ob der Bundesrat die richtige Regelungsinstanz ist, zumal die Hoheit der Kantone tangiert ist. Zudem enthält Art. 78 E-NDG so gut wie keine Anhaltspunkte, in welchem Rahmen der Bundesrat insbesondere die Dienstaufsicht durch die Kantone zu regeln hat.

Aus diesen Gründen sollen die Aufsicht in den Kantonen und ihr Verhältnis zum Bund zumindest in den wesentlichen Zügen durch die Eidg. Räte in Art. 78 E-NDG festgelegt werden. Einzelheiten, insbesondere wenn sie auch den NDB oder das VBS betreffen, können dann vom Bundesrat im Ausführungsrecht geregelt werden.

In diesem Sinn ist es auch vertretbar, dass in Art. 76 Abs. 3 Bst. b E-NDG der Bundesrat weiterhin Mindestanforderungen an die Kontrollen in den Kantonen vorschreiben kann (wie Art. 26 Abs. 3 BWIS). Die grundlegenden Zuständigkeiten soll jedoch der Gesetzgeber regeln.

### **3. Informationsrechte der GPDeI (Art. 76 und 70)**

#### **Problematik**

Bisherige Informationspflichten des Bundesrats gegenüber der GPDeI (Tarnidentitäten, Tätigkeitsverbote) sollen entgegen dem Vorschlag des Bundesrats im E-NDG nicht aufgehoben werden.

Die neue Vorgabe, die GPDeI möglichst schnell über die Erweiterung der Aufgaben des NDB gemäss Art. 3 E-NDG informieren zu müssen, hat hingegen keinen praktischen Nutzen für die Oberaufsicht. Diese Informationspflicht des Bundesrats wird nicht zu einer Selbstbeschränkung führen, welche vom E-NDG gar nicht vorgesehen wird.

#### **Anträge der GPDeI**

Art. 76 Aufsicht und Kontrolle durch den Bundesrat

*2bis (neu) Das VBS orientiert den Bundesrat und die Geschäftsprüfungsdelegation jährlich oder nach Bedarf über den Zweck und die Anzahl der Tarnidentitäten, die von Mitarbeiterinnen und Mitarbeitern des NDB oder der Sicherheitsorgane der Kantone verwendet werden. Die Zahl der neu ausgestellten Identitätspapiere ist separat auszuweisen. [wie Art. 27 Abs. 1bis BWIS]*

*2ter (neu) Der Bundesrat orientiert die Geschäftsprüfungsdelegation jährlich und nach Bedarf über Verbote von Tätigkeiten und die Ergebnisse der regelmässigen Prüfung nach Artikel 72 Absatz 3. [wie Art. 27. Abs. 1 ter BWIS]*

~~Art. 70 Abs. 4 E-NDG (streichen) Erteilt der Bundesrat einen Auftrag nach Absatz 1, so informiert er die Geschäftsprüfungsdelegation innerhalb von 24 Stunden darüber.~~

#### **Begründung**

Wie das bisherige Recht sieht der E-NDG vor, dass der Bundesrat die Beobachtungsliste nach ihrer Genehmigung an die GPDeI weiterleitet (Art. 69 Abs. 1 Bst. b E-NDG) und dass der Kontrollplan der ND-Aufsicht mit den parlamentarischen Aufsichtstätigkeiten abzustimmen ist (Art. 74 Abs. 1 E-NDG).

Im E-NDG nicht mehr explizit erwähnt sind jedoch:





- Der jährliche Bericht des Bundesrats an die GPDel über die Zahl der Tarnidentitäten und ihre Verwendung durch den NDB und die kantonalen Staatsschutzorgane (vgl. Art. 27 Abs. 1bis BWIS)
- Der jährliche Bericht des Bundesrats an die GPDel über Tätigkeitsverbote (vgl. Art. 27 Abs. 1ter BWIS)

Diese Informationen an die GPDel, die auch mit einer Aufsichtspflicht des Bundesrats verbunden sind, gehören auch ins neue Gesetz. Ein geeigneter Ort wäre Art. 76 E-NDG betreffend die Aufsicht des Bundesrats.

Art. 70 Abs. 4 E-NDG verlangt hingegen neu, dass der Bundesrat die GPDel innert 24 Stunden über die Erteilung eines Auftrags zur Wahrung wesentlicher Landesinteressen in besonderen Lagen nach Art. 3 E-NDG informiert. Gegenüber der bereits von Art. 154 Abs. 3 ParlG geregelten Praxis bietet diese Bestimmung keinen erkennbaren Mehrwert für parlamentarische Oberaufsicht.

Mit Art. 3 E-NDG würde der Gesetzgeber dem NDB in der „besonderen Lage“ umfangreiche neue Aufgabengebiete sozusagen auf Vorrat zuweisen. Gleichzeitig soll der NDB das ganze Spektrum der Informationsbeschaffungsmittel ohne besondere Vorbedingungen auch für diese Aufgaben einsetzen dürfen. Somit überlässt es der E-NDG voll und ganz dem Ermessen des Bundesrats, die Möglichkeiten von Art. 3 E-NDG voll auszuschöpfen. Auch eine umgehende Kontrolle der GPDel wäre nicht geeignet, hier eine Selbstbeschränkung, welche das Gesetz nicht vorsieht, zu bewirken. Die parlamentarische Oberaufsicht ist nach Art. 26 Abs. 4 ParlG überdies auch nicht befugt, Beschlüsse des Bundesrats aufzuheben oder zu ändern.

Zu bedenken ist auch, dass der Begriff „besondere Lage“ im Gegensatz zur „ausserordentlichen Lage“ (vgl. Art. 58 Abs. 2 BV) staatsrechtlich neu und völlig offen ist. Der E-NDG enthält keine Ansätze für eine Legaldefinition. Eine nachträgliche Kontrolle der GPDel, ob nun eine „besondere Lage“ vorlag oder nicht, wäre deshalb nicht möglich.

Da der NDB aktuell über kein Fachwissen zum Werk-, Wirtschafts- und Finanzplatz Schweiz verfügt, müsste der Bundesrat auch einen entsprechenden Personalaufbau im NDB beschliessen. Laut Botschaft bliebe dabei die Budgethoheit der eidgenössischen Räte selbstverständlich vorbehalten (Botschaft NDG, S. 37). Allenfalls wäre deshalb eine rechtzeitige Konsultation der FinDel von Belang.

#### **4. Führung durch den Bundesrat (Art. 69)**

##### ***Problematik***

Behebung eines rechtsetzungstechnischen Fehlers und einer Duplikation von Bestimmungen im gleichen Artikel.

##### ***Antrag der GPDel***

Art. 69 Abs. 2 E-NDG (streichen)

~~2 Die Dokumente im Zusammenhang mit den Aufgaben nach Absatz 1 sind nicht öffentlich zugänglich.~~



### **Begründung**

Laut Art. 69 Abs. 1 E-NDG entscheidet der Bundesrat wie bisher über den geheimen Grundauftrag (Bst. a), die vertrauliche Beobachtungsliste (Bst. b) sowie über die Auslandskontakte (Bst. f) des NDB. Die beiden letzten Regelungen werden aus dem bisherigen Verordnungsrecht (Art. 2 Abs. 2 und Art. 12 Abs. 2 V-NDB) erstmals ins Gesetz übernommen.

Beibehalten wird auch der jährliche Bericht der Bundesrats über die Bedrohungslage (bisher Art. 27 Abs. 1 BWIS). Art. 69 Abs. 2 E-NDG verbietet es jedoch, diesen Bericht zu veröffentlichen, was wohl ein rechtsetzungstechnischer Fehler sein dürfte. Da der Grundauftrag geheim und die Beobachtungsliste vertraulich ist, muss ausserdem im Gesetz nicht noch festgehalten werden, dass diese Unterlagen nicht öffentlich sind.

## **5. Aufsicht und Kontrolle durch den Bundesrat (Art. 76)**

### **Problematik**

Die Rolle des Bundesrats als oberste Aufsicht über die Bundesverwaltung (Art. 187 Abs. 1 Bst. a BV) wird im E-NDG gegenüber dem Nachrichtendienst kaum konkretisiert. Wichtige Bestimmungen aus dem bisherigen Recht wurden jedoch ersatzlos gestrichen, insbesondere die Genehmigung von Verwaltungsvereinbarungen zwischen dem NDB und Partnerdiensten durch den Bundesrat.

### **Antrag der GPDel**

*Art. 76 Abs. 1bis E-NDG (neu)*

*Der Bundesrat genehmigt vom NDB abgeschlossene zwischenstaatliche Verwaltungsvereinbarungen, die auf längere Dauer angelegt sind, substanzielle finanzielle Konsequenzen haben oder von denen der Bundesrat aus rechtlichen oder politischen Gründen Kenntnis haben sollte. Der Genehmigungsvorbehalt gilt auch für nicht schriftlich abgefasste Vereinbarungen. Die Vereinbarungen dürfen erst nach erfolgter Genehmigung vollzogen werden. [analog zu Art. 26 Abs. 2 BWIS]*

### **Empfehlung der GPDel**

Abzuklären wäre allenfalls, wie sich Art. 76 Abs. 3 Bst. a E-NDG mit den Bestimmungen des Finanzkontrollgesetzes verträgt und wie die FinDel davon betroffen wird.

### **Begründung**

Aus dem bisherigen Recht wurden drei Aufsichtsaufgaben des Bundesrats gestrichen:

- Die Genehmigung von Verwaltungsvereinbarungen zwischen dem NDB und Partnerdiensten durch den Bundesrat vor ihrem Vollzug (Art. 8 ZNDG i.V. Art. 26 Abs. 2 BWIS).
- Die jährliche Kenntnisnahme der Zahl der Tarnidentitäten und ihrer Verwendung im NDB und den Kantonen durch den Bundesrat (vgl. Antrag unter Ziff. 3).
- Die jährliche Überprüfung durch den Bundesrat, ob ein Tätigkeitsverbot aufrechterhalten werden soll (vgl. Antrag unter Ziff. 3).

Die Genehmigung von Verwaltungsvereinbarungen zwischen dem NDB und Partnerdiensten durch den Bundesrat verlangt im bisherigen Recht vom Bundesrat eine gewisse Kontrolle über



die Ausübung der von ihm genehmigten Auslandkontakte des NDB. So hätte der Bundesrat beispielsweise eine Vereinbarung des NDB mit der NSA, die laut Medienauskünften des VBS eine Voraussetzung für einen Informationsaustausch zwischen beiden Diensten gewesen wäre, vorgängig genehmigen müssen.

Im Rahmen der Pa. Iv. Hofmann (07.404) hatte die GPDel dafür gesorgt, dass die ursprünglich im BWIS verankerte Bewilligungspflicht des Bundesrates für solche Verwaltungsvereinbarungen auch für den NDB eingeführt wurde. Die GPDel wacht darüber, dass diese Bestimmung eingehalten wird (Jahresbericht GPDel 2013 vom 31.1.2014, Ziff. 4.1.1, S. 59). Die im Antrag der GPDel vorgeschlagene Bestimmung beschränkt die Genehmigungspflicht des Bundesrats auf bedeutsame Vereinbarungen. Gleichzeitig wird klargestellt, dass die Genehmigungspflicht nicht umgangen werden kann, wenn der NDB darauf verzichtet, die Vereinbarung schriftlich festzuhalten oder zu unterzeichnen.

Die im E-NDG gestrichene Vorschrift, dass sich der Bundesrat jährlich mit der Verwendung von Tarnidentitäten befassen muss, sorgte bisher für eine übergeordnete Kontrolle, bei der die Verwendung dieser Mittel überprüft und auf das Notwendige beschränkt wurde. Die entsprechende Bestimmung aus dem BWIS soll deshalb in den neuen Absatz 2bis von Art. 76 E-NDG übernommen werden (vgl. Anträge in Ziff. 3).

Nach Art. 72 Abs. 3 E-NDG soll allein das VBS (oder ein anderes antragstellendes Departement) regelmässig die Notwendigkeit eines Tätigkeitsverbotes überprüfen. Wie nach dem bisherigen Art. 9 Abs. 3 BWIS sollte aber weiterhin der Bundesrat diese Beurteilung gegenüber der GPDel vertreten müssen (vgl. Antrag unter Ziff. 3 betr. Art. 76 Abs. 2ter E-NDG).

Die übrigen Bestimmungen des Artikels begründen keine eigentlichen Aufsichtsaufgaben des Bundesrats, sondern Regelungskompetenzen, die besser in den thematisch relevanten Artikeln aufgehoben wären.

Nach Art. 76 Abs. 3 Bst. a E-NDG soll der Bundesrat die Finanzaufsicht in den Geheimbereichen des NDB regeln. Nicht klar ist, wie sich dieser Regelungsauftrag mit den Bestimmungen des Finanzkontrollgesetzes verträgt und wie die FinDel davon betroffen wird.

## **6. Konsultation des SiA (Art. 29)**

### ***Problematik***

Für eine wirksame Oberaufsicht ist es notwendig, dass die Konsultation von EDA und EJPD für die Freigabe einer genehmigungspflichtigen Beschaffungsmassnahme schriftlich erfolgt. Die Organisationsautonomie des Bundesrats sollte hingegen nicht beschränkt werden, indem ein einziger Ausschuss des Bundesrats erstmals auf Gesetzesstufe verankert wird. Denn die Ausschüsse des Bundesrats haben keine Entscheidungsbefugnisse.

### ***Antrag der GPDel***

#### **Art. 29 Freigabe**

1 Liegt die Genehmigung der Beschaffungsmassnahme vor, so entscheidet die Chefin oder der Chef des VBS, nach vorheriger Konsultation *des EDA und des EJPD*, über die Freigabe zur Durchführung. *Fälle von besonderer Bedeutung können dem Bundesrat vorgelegt werden.*

2 *Das Konsultationsverfahren ist schriftlich zu führen.*



### **Begründung**

Nach dem bisherigen Recht obliegt es dem Bundesrat allein zu entscheiden, welche Ausschüsse er bestellen will (Art. 23 Abs. 1 RVOG). Es stellt sich deshalb die Frage, ob mit Art. 29 E-NDG die Existenz des SiA im Gesetz festgeschrieben und seine Zusammensetzung präjudiziert werden soll. Dies kann vermieden werden, indem die Departemente EDA und EJPD anstelle des SiA erwähnt werden. In Bezug auf die Kontrolle des Nachrichtendienstes würde sich hingegen materiell nichts ändern.

Aus dem E-NDG geht nicht hervor, welche Informationen der Chef VBS den beiden anderen Bundesräten im Rahmen der Konsultation vorlegen muss. Insbesondere ist unklar, ob sie im gleichen Umfang wie das BVGer informiert werden müssen. Damit die beigezogenen Departemente ihre Mitwirkung in der Gestalt der Konsultation ausüben können, muss das Verfahren schriftlich geführt werden, analog zu den Ermächtigungsverfahren (Art. 3 Bst. a OV-EJPD, Organisationsverordnung für das EJPD), welche grundsätzlich in die Kompetenz des EJPD fallen.

## **7. Aufsicht durch das VBS (Art. 74)**

### **Problematik**

Um auf Stufe Departement eine durchgängige politische Kontrolle auch der sensitivsten Tätigkeiten des Nachrichtendienstes sicherzustellen, sollte der Vorsteher VBS mindestens einmal pro Jahr von den Beschaffungsaktivitäten, die nicht bereits durch das Gesetz seiner Genehmigung unterworfen sind, Kenntnis nehmen müssen. Dies damit er seine departementale Aufsichtsfunktion wahrnehmen kann.

### **Antrag der GPDel**

Art. 74 Abs. 5 E-NDG (neu)

*Der Chef oder die Chefin VBS erhält jährlich einen Bericht, in welchem der NDB die Angemessenheit der Weiterführung der nicht genehmigungspflichtigen Operationen beurteilt.*

### **Begründung**

Unter dem bisherigen Recht muss der Vorsteher VBS einmal jährlich zu jeder nachrichtendienstlichen Operation, welche der NDB alleine oder zusammen mit kantonalen oder ausländischen Partnern durchführt, eine Beurteilung des NDB zur Frage einholen, ob die Weiterführung der Operation gerechtfertigt ist (Art. 24 Abs. 5 V-NDB).

Eine solche Kenntnisnahme ist eine notwendige Voraussetzung für die durchgängige politische Kontrolle auf Stufe Departement auch der sensitivsten Tätigkeiten des Nachrichtendienstes, v.a. auch jener im Ausland.

Der von der GPDel vorgeschlagene neue Absatz 5 würde insbesondere die Informationsbeschaffung, für die nicht bereits eine Genehmigungspflicht des Vorstehers VBS oder ein besonderes Kontrollorgan (z.B. Funkaufklärung) im Gesetz vorgesehen ist, abdecken.

Nach Art. 74 Abs. 2 E-NDG 2 ist die vom VBS einzusetzende interne Aufsichtsinstanz in der Erfüllung ihrer Kontrollaufgaben weisungsungebunden. Eine solche Garantie fehlte im bisherigen Recht. Damit hat der Bundesrat die Empfehlung 11 des Inspektionsberichts der GPDel zur Informatiksicherheit im NDB - soweit auf Stufe Rechtsetzung möglich - erfüllt. Darin hatte die GPDel den Chef VBS aufgefordert, für die Respektierung der Einsichtsrechte der



ND-Aufsicht zu sorgen. Insbesondere dürfe der NDB diese Informationsrechte weder alleine noch im Einverständnis mit dem Departementsvorsteher beschränken können.

## **8. Aufgaben des NDB (Art. 3, 6, 16, 19, 26, 37 und 70)**

### ***Problematik***

Im Vergleich zum bisherigen Recht sieht der E-NDG eine substanzielle Ausweitung der gesetzlichen Aufgaben des NDB vor. Insbesondere soll der NDB seine neuen Instrumente auch dann einsetzen können, wenn die Schweiz und ihre Institutionen nicht direkt bedroht sind, sondern nur mittelbar, beispielsweise durch die Schwächung eines Wirtschaftssektors. Dies ist verfassungsrechtlich problematisch, da sich der Staatsschutz mangels einer expliziten Verfassungsgrundlage bereits heute auf eine ungeschriebene, inhärente Verfassungskompetenz abstützen muss.

### ***Anträge der GPDel***

#### Streichung folgender Bestimmungen:

Art. 3; Art. 6 Abs. 1 Bst. d; Art. 16 Abs. 2 Bst. d; Art. 37 Abs. 2 Bst. b; Art. 70 E-NDG.

#### Streichung der Referenzen auf Art. 3 E-NDG in:

Art. 19 Abs. 1; Art. 26 Abs. 1 Bst. c E-NDG.

### ***Begründung***

Art. 6 E-NDG enthält eine Aufzählung der gesetzlichen Aufgaben des NDB. Darunter fallen die bisherigen Aufgaben des NDB im Ausland (Beschaffung von sicherheitspolitisch bedeutsamen Informationen) und die bisher im BWIS festgelegten Aufgaben (Terrorismus, gewalttätiger Extremismus, verbotener Nachrichtendienst, Proliferation).

Die Aufgaben zum Schutz der Schweiz vor Spionage durch private und staatliche ausländische Akteure (Art. 6 Abs. 1 Bst. a Ziff. 2 E-NDG) werden zusätzlich in Art. 19 Abs. 2 Bst. b E-NDG konkretisiert:

- Abwehr von politischem Nachrichtendienst (Art. 272 StGB);
- Abwehr von wirtschaftlichem Nachrichtendienst (Art. 273 StGB). Darunter fällt beispielsweise der Diebstahl von Bankdaten, wenn er zugunsten eines ausländischen Auftraggebers erfolgt.
- Abwehr von militärischem Nachrichtendienst (Art. 274 StGB).

Weiter klärt der NDB auch nachrichtendienstliche Aktivitäten auf dem Gebiet der Schweiz auf, die gegen fremde Staaten gerichtet sind (Art. 301 StGB). Damit soll auch die Neutralität der Schweiz gewahrt werden.

Neu hingegen ist die Ausdehnung des Staatsschutzes auf die Abwehr von Angriffen auf kritische Infrastrukturen (vgl. Art. 6 Abs. 1 Bst. a Ziff. 4 E-NDG). Während beispielsweise ein Zusammenbruch der Informations- und Kommunikationsinfrastruktur die Funktionsweise von Staat, Wirtschaft und Gesellschaft in Frage stellen kann, dürfte hingegen ein Brand in einem Autobahn- oder Eisenbahntunnel nie vergleichbare Auswirkungen haben. Zu beachten wären hier insbesondere die Zuständigkeiten anderer Bundesstellen oder solche der Kantone.





Fundamental neu gegenüber dem bisherigen Recht ist auch Art. 3 E-NDG, auf den in Art. 6 Abs. 1 Bst. d E-NDG verwiesen wird. Mit Art. 3 E-NDG überlässt es der Gesetzgeber dem Ermessen des Bundesrats, alle im Gesetz vorgesehenen Beschaffungsmittel einzusetzen, um „wesentliche Landesinteressen“ (Aussenpolitik, Interessen des Werk-, Wirtschafts- und Finanzplatzes, etc.) zu schützen.

Da insbesondere eine allgemeine Aufgabe wie der Schutz des Werk-, Wirtschafts- und Finanzplatzes eine Bedrohung betrifft, die den Staat bloss mittelbar und nicht in seiner eigentlichen Existenz gefährdet, stellt sich die Frage nach der Verfassungsmässigkeit von Art. 3 E-NDG.

In der Praxis wie auch in der Lehre gilt zwar als gesichert, dass der Bund die inhärente Kompetenz hat, Massnahmen zu seinem Schutz und zum Schutz seiner Organe und Institutionen zu treffen; er hat den Bestand des gesamtschweizerischen Gemeinwesens zu gewährleisten und zu sichern und für die Abwehr von Gefahren zu sorgen, die dieses Gemeinwesen existenziell bedrohen. Bezüglich des Umfangs, der Tragweite und der Grenzen dieser inhärenten Bundeszuständigkeit bestünde aber Unsicherheit, schrieb der Bundesrat in seinem Bericht zum Postulat Malama. Der Bundesrat vertrat deshalb die These, dass die Staatsschutzfähigkeit des Bundes auf eine explizite Verfassungsnorm abgestützt werden sollte (Bericht zu Po. Malama, BBI 2012 4597).

Da der Gesetzgeber bisher auf die Schaffung einer expliziten Verfassungsgrundlage für den Staatsschutz verzichtet hat, kann sich der E-NDG, wie bisher das BWIS auch, bloss auf inhärentes Verfassungsrecht abstützen.

Inhärentes Verfassungsrecht ist aufgrund seiner Unbestimmtheit jedoch mit grösster Zurückhaltung zu bemühen. Dies gilt insbesondere für die Abwehr von Bedrohungen, die den Staat bloss mittelbar, z.B. durch Schwächung eines Wirtschaftssektors, in seiner Funktionstüchtigkeit treffen (Bericht zum Po. Malama, BBI 2012 4581). Art. 3 E-NDG erscheint deshalb aus verfassungsrechtlicher Sicht bedenklich.

Die GPDel erinnert daran, dass Art. 184 und 185 BV dem Bundesrat bereits heute erlauben, befristete Massnahmen zur Wahrung der Landesinteressen und um schweren Störungen der inneren und äusseren Sicherheit zu begegnen, zu treffen. Dies ist auch im Bereich des Nachrichtendienstes möglich, wobei die gewählte Massnahme verhältnismässig, geeignet und, mangels milderer Alternative, notwendig sein muss.

Erwähnenswert ist in diesem Zusammenhang, dass die BWIS-II-Vorlage von 2007, welche vom Parlament abgewiesen wurde, keine Ausweitung der nachrichtendienstlichen Aufgaben vorgesehen hatte.

Weiter ist auch zu berücksichtigen, dass die Wahrnehmung solch neuer Aufgaben einen substanziellen Bedarf an zusätzlichen Ressourcen für den NDB zur Folge haben kann (vgl. Ziff. 31).

## **9. Auskunftspflichten von Behörden (Art. 19 und 20)**

### ***Problematik***

Nach dem E-NDG kann der NDB im Vergleich zum geltenden Recht von mehr Stellen und in mehr Fällen Auskünfte erhalten. Gleichzeitig werden die Auflagen reduziert, die für ein Gesuch des NDB erfüllt sein müssen. Auch das Berufsgeheimnis soll nicht mehr gewahrt bleiben und Schranken bei der Weitergabe der erhaltenen Auskünfte an die Strafverfolgungsbehörden werden aufgehoben. Die diesbezüglichen geltenden Bestimmungen des BWIS sollen jedoch beibehalten werden.



### **Anträge der GPDel**

Art. 19 Abs. 1 E-NDG: Behörden ... ~~dienen~~ notwendig sind. (wie Art. 13a Abs. 1 BWIS)

Art. 19 Abs. 5 E-NDG (neu): Der Bundesrat bestimmt in einer Verordnung die Organisationen, die zu Auskünften verpflichtet sind. Darunter fallen namentlich Organisationen des öffentlichen und privaten Rechts, die nicht der Bundesverwaltung angehören, soweit sie Erlasse oder erstinstanzliche Verfügungen im Sinne von Artikel 5 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 erlassen oder soweit sie ihnen übertragene Vollzugsaufgaben des Bundes erfüllen; ausgenommen sind Kantone. [wie Art. 13 Abs. 3 BWIS]

Art. 19 Abs. 6 E-NDG (neu): Werden dem NDB durch Auskünfte nach Absatz 1 strafbare Handlungen der Person, über die Auskunft eingeholt wurde, oder von Drittpersonen bekannt, so dürfen die Erkenntnisse den Strafverfolgungsbehörden nur zur Abklärung schwerer Straftaten zur Verfügung gestellt werden. [wie Art. 13a Abs. 4 BWIS]

Art. 20 Abs. 1 Bst a E-NDG: ~~Gerichte~~, Strafverfolgungsbehörden sowie Behörden des Straf- und Massnahmenvollzugs;

Art. 20a Berufsgeheimnis (neu)

Bei Auskünften nach den Artikeln 19 oder 20 bleibt das gesetzlich geschützte Berufsgeheimnis gewahrt. [wie Art. 13d BWIS]

### **Empfehlung**

Es sollte abgeklärt werden, ob Bundesstellen im Bereich der humanitären Hilfe oder der Auslandshilfe von der Auskunftspflicht auszuschliessen sind. Sie laufen nämlich aufgrund der Auskunftspflicht Gefahr, im Ausland als Agenten des NDB betrachtet zu werden.

### **Begründung**

Art. 19 und 20 E-NDG regeln die Amtshilfe an den NDB und die damit verbundene Aufhebung des Amtsgeheimnisses, welchem die betroffenen Stellen des Bundes und der Kantone unterworfen sind.

Art. 19 E-NDG erlaubt es dem NDB, zum Erkennen einer konkreten Bedrohung Auskünfte zu verlangen. Im Vergleich zum bisherigen Art. 13a BWIS wird der Anwendungsbereich jedoch auf alle Aufgaben des NDB ausgeweitet:

- Die Auskunftspflicht dient nicht mehr allein zum Erkennen von Bedrohungen durch Terrorismus, Spionage oder Proliferation, sondern neu auch von Bedrohungen durch gewalttätigen Extremismus oder für kritische Infrastrukturen.
- Bisher durften nur Informationen verlangt werden, die „notwendig sind“ (Art. 13a Abs. 1 BWIS), um die Bedrohung zu erkennen oder abzuwehren. Nach Art. 19 E-NDG genügt es nunmehr, wenn sie dazu „dienen“.

Gleichzeitig fehlen in Art. 19 E-NDG die bisherigen Bestimmungen, die zur Rechtssicherheit und zum Rechtsschutz beitragen:

- Der Bundesrat bestimmt nicht mehr in einer Verordnung die Organisationen, denen der Bund Aufgaben übertragen hat und die zu Auskünften verpflichtet sind (Art. 13a Abs. 3 BWIS). Heute sind dazu in Anhang 5 V-NDB folgende Organisationen aufgeführt: WEKO, SNF, ESTI, SBB, SBB Cargo, Post und Billag.



- Weiter sieht der E-NDG keine Einschränkung der Weitergabe von erhaltenen Auskünften an die Strafverfolgungsbehörden mehr vor. Art. 13a BWIS erlaubt dies nur zur Abklärung schwerer Straftaten. Dieser Mangel wird auch nicht durch Art. 59 Abs. 3 E-NDG kompensiert, da dort nur die Weitergabe von Informationen aus genehmigungspflichtigen Beschaffungsmassnahmen nach Art. 25ff E-NDG geregelt wird.

Im E-NDG fehlt der Schutz des Berufsgeheimnisses, der im BWIS noch bei den Auskunftspflichten vorgesehen war. So war gemäss dem bisherigen Art. 13d BWIS beispielsweise ein Kantonsarzt zu allgemeinen Auskünften verpflichtet, nicht aber zu Auskünften über sein unter die ärztliche Schweigepflicht fallendes Wissen (BWIS-II-Zusatzbotschaft vom 27.10.2010, BBI 2010 7878).

Art. 20 E-NDG weitet die bisherige allgemeine Auskunftspflicht nach Art. 13 BWIS auf verschiedene zusätzliche Behörden aus. Es sind dies die Gerichte, die Behörden des Straf- und Massnahmenvollzugs und die Behörden, die Informatiksysteme betreiben sowie die Finanzmarktaufsicht.

Die Ausweitung der generellen Auskunfts- und Meldepflicht auf alle Gerichte ist wegen der Gewaltenteilung besonders problematisch. Zu erwähnen ist, dass die Gerichte erst nach der Vernehmlassung zum E-NDG als auskunfts- und meldepflichtige Behörden in das NDG aufgenommen wurden und sich dafür in den Erläuterungen keine Begründung findet.

Aufgrund der Streitfallregelung von Art. 21 Abs. 2 E-NDG würde es überdies neu möglich sein, dass das BVGer abschliessend darüber entscheidet, ob z.B. das BGer dem NDB Auskunft erteilen müsste.

## **10. Meldungen und Auskünfte von Dritten (Art. 22)**

### ***Problematik***

Damit Auskünfte von Dritten an den NDB effektiv freiwillig sind, muss der NDB klar als Fragesteller erkennbar sein. Eine Verschleierung mittels Legende (vgl. Art. 17) widerspricht dieser Auflage. Die Anwendbarkeit der Bestimmung soll auf das Inland beschränkt werden. Dies entspricht dem Ansatz des E-NDG, die Informationsbeschaffung im Ausland nicht näher zu regeln.

### ***Antrag der GPDel:***

Art. 22 Meldungen und Auskünfte von Dritten *im Inland*

3 Er macht die um Auskunft ersuchte Person darauf aufmerksam, dass sie freiwillig Auskunft gibt; ~~ausgenommen ist die Informationsbeschaffung unter Verwendung einer Legende.~~

### ***Begründung***

Nach Art. 22 Abs. 3 E-NDG soll der NDB die betroffenen Person darauf hinweisen müssen, dass ihre Auskunft freiwillig ist.

Ein Problem ergibt sich jedoch beim Einholen von Auskünften, wenn die Zugehörigkeit zum Nachrichtendienst mittels einer Legende verschleiert wird. In diesem Fall erlaubt es Art. 22 Abs. 3 E-NDG, auf den obligatorischen Hinweis auf die Freiwilligkeit der Auskunft zu verzichten. Dies wird jedoch dann besonders problematisch, wenn die Legende so gewählt wird, dass die befragte Person den Eindruck erhält, sie sei zur Auskunft verpflichtet.



Für Vertreter des Nachrichtendienstes dürfte es vor allem wichtig sein, dass sie sich bei der Informationsbeschaffung im Ausland nicht als solche zu erkennen geben müssen.

Würde der Geltungsbereich von Art. 22 E-NDG explizit auf das Inland beschränkt werden, entfielen diese Problematik. Damit würde auch dem Ansatz des E-NDG entsprochen, die Informationsbeschaffung im Ausland nicht näher zu regeln.

Muss die Identität des Mitarbeiters des NDB im Inland geschützt werden, kann er dazu eine Tarnidentität verwenden, die gemäss den Erläuterungen zu Art. 22 Abs. 3 E-NDG nicht „zwangsläufig mit einer Verschleierung der Zugehörigkeit zum NDB verbunden sein muss“ (Botschaft NDG, S. 56).

## **11. Anhaltung von Dritten (Art. 23)**

### ***Problematik***

Art. 23 E-NDG, dessen Überschrift unvollständig und deshalb missverständlich ist, ermächtigt Mitarbeitende des NDB, potentiell jede Person anzuhalten und sie an einen vom NDB gewählten Ort zu bringen, in der Botschaft ist die Rede von einem „geschützten Ort“, um sie dort kurz zu befragen.

Eine Höchst- oder Gesamtdauer für diese „Anhaltung“ wird auf Gesetzesstufe nicht festgelegt. In der Botschaft ist die Rede davon, dass die Gesamtdauer in Analogie zur Abgrenzung zwischen der polizeilichen Anhaltung und der polizeilichen Festnahme unter drei Stunden liegen soll.

Damit werden den Mitarbeitenden des NDB Kompetenzen verliehen, welche das BWIS in dieser Form nicht kennt und die somit ausschliesslich der Polizei zur Aufklärung von Straftaten zustehen (vgl. Art. 215 StPO, polizeiliche Anhaltung).

Bei der polizeilichen Anhaltung (Art. 215 StPO) handelt es sich um eine Zwangsmassnahme. Obwohl nach Art. 23 Abs. 1 E-NDG die Auskunft freiwillig sein soll (Verweisung auf Art. 22 E-NDG), kann die neue Bestimmung, welche nicht Teil der Vernehmlassung war, leicht mit der gleichen Wirkung wie eine polizeiliche Zwangsmassnahme eingesetzt werden.

### ***Antrag der GPDel***

Art. 23 E-NDG streichen.

### ***Begründung***

Art. 23 E-NDG orientiert sich laut Botschaft explizit an Art. 215 StPO („Polizeiliche Anhaltung“) und gibt dem NDB die gleichen Kompetenzen. Der Artikel mit dem Titel „Identifikation und Befragung“ gelangt damit in die Nähe einer polizeilichen Festnahme (vgl. Botschaft StPO vom 21.12.2005, BBI 2006 1224).

Im Gegensatz zur Festnahme, die sich gegen eine Person richtet, gegen welche ein Verdacht vorliegt, soll durch die Anhaltung die Identität einer Person festgestellt und geklärt werden, ob sie eine Straftat begangen hat oder sonst damit in Zusammenhang zu bringen ist. Der Anhaltung liegt also die Situation zugrunde, dass zuerst geklärt werden muss, wer eines Delikts verdächtig ist.

Ergibt sich nach einem kurzen Aufenthalt auf dem Polizeiposten kein Verdacht, ist die Person sofort zu entlassen, anderenfalls ist eine Festnahme anzuordnen. Weil bereits eine vorläufige Festnahme (Art. 217 StPO) ohne die Anordnung eines höheren Polizeiangehörigen des



Bundes oder der Kantone höchstens während 3 Stunden aufrecht erhalten werden darf, schliesst die Botschaft daraus, dass eine Anhaltung nach Art. 215 StPO „insgesamt deutlich weniger als [diese] 3 Stunden“ dauern darf (Botschaft StPO, BBl 2006 1224).

Aus den Erläuterungen zu Art. 23 E-NDG muss geschlossen werden, dass der NDB die angehaltene Person an einen Ort seiner Wahl bringen kann, „beispielsweise an einen geschützten Ort“, wenn die konkreten Umstände es rechtfertigen. Bei diesem Ort handelt es sich also nicht zwingend um einen Polizeiposten, ansonsten dies erwähnt worden wäre. Laut Botschaft kann die Gesamtdauer der Anhaltung „bis zu wenigen Stunden dauern“, müsse aber unter 3 Stunden liegen“ (Botschaft NDG, S. 57). Dies ist jedoch mehr als die „deutlich weniger als 3 Stunden“, die im Rahmen der StPO gelten (Botschaft StPO, BBl 2006 1224).

Während die Polizei gestützt auf Art. 215 StPO die Bewegungsfreiheit von Personen nur in Ausübung ihrer Ermittlungsbefugnisse einschränken darf, hat der NDB für die gleiche Massnahme freies Ermessen, solange er dies als zweckmässig für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit erachtet (Art. 6 Abs. 1 Bst. a E-NDG). Es braucht dafür weder einen externen Anlass noch eine konkrete Bedrohung, wie sie beispielsweise als Voraussetzung für die besonderen Auskunftspflichten von Behörden oder Privater (Art. 19 und Art. 24 E-NDG) verlangt werden. A priori kann davon jede Person betroffen sein, die sich auf Schweizer Staatsgebiet aufhält.

Art. 23 Abs. 2 E-NDG stipuliert, dass die angehaltene Person nach den Modalitäten von Art. 22 E-NDG befragt werden kann, d.h. auch völlig frei ist, ihre Auskunft zu verweigern.

Diese gesetzliche Garantie dürfte aber in der Praxis schnell an Wirksamkeit verlieren, wenn eine Person für bis zu drei Stunden an einen geheimen Ort verbracht werden kann und deshalb konkrete Nachteile, beispielsweise einen verpassten Linienflug oder anderweitige Widrigkeiten in Kauf nehmen muss. Für eine solche Konstellation fehlt zudem im E-NDG jede Möglichkeit zur nachträglichen Beschwerde.

Erwähnenswert ist ausserdem, dass der ganze Art. 23 E-NDG erst nach Abschluss des Vernehmlassungsverfahrens Eingang in das Gesetz fand und somit nie öffentlich zur Diskussion gestellt wurde.

## **12. Besondere Auskunftspflicht Privater (Art. 24)**

### ***Problematik***

Gegenüber dem bestehenden Recht verringert Art. 24 E-NDG nicht nur den Rechtsschutz, sondern verzichtet auch auf die Regelung der Weitergabe der erhaltenen Informationen an die Strafverfolgungsbehörden. In der Botschaft fehlt auch eine Beurteilung, wie sich die Ausweitung der Auskunftspflichten auf die Grundrechte nicht nur der betroffenen Firmen, sondern auch auf diejenigen Personen, zu denen Bild und Videodaten gesammelt werden, auswirkt.

### ***Antrag der GPDeI***

*Art. 24 Abs. 3 (neu) Werden dem NDB durch Auskünfte nach Absatz 1 strafbare Handlungen der Person, über die Auskunft eingeholt wurde, oder von Drittpersonen bekannt, so dürfen die Erkenntnisse den Strafverfolgungsbehörden nur zur Aufklärung schwerer Straftaten zur Verfügung gestellt werden. [wie Art. 13c Abs. 3 BWIS]*





### **Empfehlung der GPDeI**

Es sollte abgeklärt werden, wie sich die Ausweitung der Auskunftspflichten Privater auf die Grundrechte (Video-Überwachung) und den Rechtsschutz auswirkt. Dies könnte mit einer Ergänzung des Gutachtens (Gutachten von Prof. Biaggini vom Juni 2009, VPB 4/2009, S. 290-295), das die RK-N zur BWIS-II-Vorlage verlangt hatte, bewerkstelligt werden.

### **Begründung**

Art. 24 E-NDG übernimmt die Auskunftspflicht der gewerbsmässigen Transporteure, die mit der BWIS-II-Revision eingeführt wurde (Art. 13c BWIS).

Im Gegensatz zum BWIS soll die Auskunftspflicht neu auch für alle privaten Betreiber von Sicherheitsinfrastrukturen gelten. Als Beispiele nennen die Erläuterungen Videoüberwachungs- oder Zutrittsanlagen in den Bereichen Verkehr oder Verkauf). Gleichzeitig wie in Art. 19 E-NDG wird die Voraussetzung für eine Auskunft erleichtert.

Im Vergleich zum BWIS schränkt der E-NDG zudem die Rechte der betroffenen Personen ein:

- Keine Einschränkung der Weitergabe an die Strafverfolgungsbehörden (Art. 13c Abs. 3 BWIS).
- Neu verliert das Ergreifen eines Rechtsmittels die aufschiebende Wirkung (Art. 79 Abs. 2 E-NDG).

Für die BWIS-II-Vorlage waren die möglichen Eingriffe, welche die Auskunftspflichten der gewerbsmässigen Transporteure in die Grundrechte des Persönlichkeitsschutzes (Art. 13 BV, Art. 8 EMRK) und der Wirtschaftsfreiheit (Art. 27 BV) bringen können, eingehend beurteilt worden.

Eine solche Beurteilung fehlt für die neuen Auskunftspflichten der Betreiber von Sicherheitsinfrastrukturen in der Botschaft zum E-NDG vollständig, obwohl durch die Herausgabe von Bild- und Videoaufnahmen aus dem öffentlichen und nicht-öffentlichen Raum potentiell viel mehr Personen betroffen sind und weiterführende Erkenntnisse über das Verhalten von Personen gewonnen werden können als durch die Auskünfte privater Transporteure.

## **13. Verfahren für genehmigungspflichtige Beschaffungsmassnahmen (Art. 28 und 31a)**

### **Problematik**

Das Verfahren für die Informationsbeschaffung nach Art. 25ff E-NDG orientiert sich an den geheimen Überwachungsmassnahmen nach Art. 269ff StPO. Dabei wurde jedoch dem Unterschied zwischen Strafverfolgung und Nachrichtendienst zu wenig Rechnung getragen, während verschiedene Regelungen aus der Strafverfolgung, die auch für die nachrichtendienstliche Beschaffung relevant sind, im E-NDG zu wenig berücksichtigt wurden.

### **Anträge der GPDeI**

Art. 28 Abs. 1 Bst. a E-NDG (Änderung): *der Angabe des spezifischen Ziels der Beschaffungsmassnahme und der Begründung ihrer Notwendigkeit sowie der Erläuterung, warum bisherige Abklärungen erfolglos waren;*

Art. 28 Abs. 2bis E-NDG (neu): *Der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts genehmigt eine beantragte Beschaffungsmassnahme nicht, wenn eine solche Massnahmen bereits aufgrund eines Strafverfahrens gegen die betroffene*



*Personen nach Absatz 1 Buchstabe b bewilligt worden ist und die Strafuntersuchung einen Zusammenhang zur konkreten Bedrohung aufweist, welche die Beschaffungsmassnahme des NDB abklären soll. Die zuständigen Zwangsmassnahmengerichte erteilen dem Bundesverwaltungsgericht die notwendigen Auskünfte.*

**Art. 31a E-NDG (Beschränkung der Datenbearbeitung) (neu)**

*1 Der NDB stellt sicher, dass Personendaten aus genehmigungspflichtigen Beschaffungsmassnahmen, die keinen Bezug zu der die Anordnung begründenden Bedrohung aufweisen, nicht bearbeitet und spätestens innert 30 Tagen nach Beendigung dieser Massnahmen vernichtet werden. [wie 18h E-BWIS-II, vgl. Antrag GPDel zu Ziff. 26]*

*2 Bei der Überwachung einer Person, die einer in den Artikeln 170 –173 StPO genannten Berufsgruppe angehört, sind Informationen, die keinen Bezug zu der die Anordnung begründenden Bedrohung aufweisen, unter der Leitung des Bundesverwaltungsgerichts auszusondern und zu vernichten. Bei der Überwachung anderer Personen sind Informationen, über welche eine in den Artikeln 170–173 genannte Person das Zeugnis verweigern könnte, ebenso zu vernichten. [analog zu Art. 271 StPO]*

**Begründung**

Das Genehmigungsverfahren für die besonderen Beschaffungsmassnahmen gemäss Art. 25ff E-NDG orientiert sich am Verfahren, das für die geheimen Überwachungsmassnahmen der Strafverfolgungsbehörden gilt (Art. 269ff StPO).

Analog zur StPO nennt Art. 26 Abs. 1 Bst. c E-NDG unter den zwingenden Voraussetzungen für den Einsatz bewilligungspflichtiger Mittel die Erfolglosigkeit bisheriger Abklärungen. In der Strafverfolgung erscheint dies als geeignetes Kriterium, um den Einsatz von Überwachungsmassnahmen als ‚ultima ratio‘ zu rechtfertigen. Ausgangspunkt ist nämlich immer eine erfolgte Straftat oder zumindest ein dringender Verdacht, dass eine solche begangen wurde (Art. 269 Abs. 1 Bst. a StPO). Fehlen Hinweise auf die Täterschaft, kann dies plausibel damit erklärt werden, dass die Täter ihr Vorgehen so gut verborgen haben, dass es nur mit sehr weitgehenden Ermittlungsmassnahmen aufgedeckt werden kann.

Bei der nachrichtendienstlichen Informationsbeschaffung hingegen kann die Erfolglosigkeit bisheriger Abklärungen ihren Grund aber auch darin haben, dass die vermutete Bedrohung gar nicht existiert (vgl. Gutachten von Prof. Biaggini, S. 263). Dieser unterschiedlichen Ausgangslage sollte im E-NDG Rechnung getragen werden.

Bei der Genehmigung ist es deshalb unerlässlich, dass der NDB gegenüber dem BVGer erklären muss, welche Beschaffungsmassnahmen er bereits unternommen hat und wie sich deren Erfolglosigkeit erklären lässt.

Wie die StPO erlaubt auch der E-NDG Personen, die dem Berufsgeheimnis unterstehen (171–173 StPO), mit genehmigungspflichtigen Beschaffungsmassnahmen zu überwachen. Solche Personen dürfen gemäss E-NDG zwar unter gewissen Umständen (Drittpersonen gemäss Art. 27 Abs. 2 E-NDG) nicht überwacht werden, es fehlt aber eine Regelung analog zu Art. 271 StPO, welche die Verwendung von Informationen, die dem Berufsgeheimnis unterliegen, regelt.

Nach den Erläuterungen „geht ein allfälliges Strafverfahren und in dessen Rahmen verfügte Überwachungsmassnahmen den Informationsbeschaffungsmassnahmen nach dem E-NDG vor“ (Botschaft NDG, S. 59). Der E-NDG regelt aber nicht die Frage, wie das BVGer erkennen kann, dass gegen eine Person bereits ein Strafverfahren läuft, um deshalb einer Massnahme des NDB die Genehmigung zu verweigern.



In ihrem Mitbericht zur ursprünglichen BWIS-II-Vorlage, welcher am 29. Februar 2008 an die RK-N ergangen war, hatte die GPDel angeregt, dass der präventive Staatschutz keine genehmigungspflichtige Informationsbeschaffungsmittel einsetzen kann, wenn bereits gerichtspolizeiliche Ermittlungen gegen die gleiche Person im Gange sind. Damit sollte verhindert werden, dass Strafverfolgung und Nachrichtendienst die gleichen Personen abhören oder gleichzeitig in den Computer der gleichen Person einzudringen versuchen.

Anders als die StPO enthält der E-NDG keine Pflicht, beschaffte Informationen zu vernichten, wenn sie keinen Bezug zum genehmigten Ziel der Beschaffungsmassnahme haben (Art. 276 StPO). Die BWIS-II-Vorlage von 2007 hatte demgegenüber noch verlangt, dass solche Personendaten spätestens innert 30 Tagen nach Einstellung der Massnahme vernichtet werden müssen (Art. 18 h E-BWIS).

In der BWIS-II-Vorlage von 2007 war hingegen der Einsatz von Ortungsgeräten (z.B. GPS) nach Art. 25 Abs. 1 Bst. b E-NDG und das Durchsuchen von Räumlichkeiten, Fahrzeugen oder Behältnissen nach Art. 25 Abs. 1 Bst. e E-NDG nicht vorgesehen. Das Durchsuchen von Räumen und Fahrzeugen wurde sogar explizit u.a. mit dem Ziel, mit der Vorlage „die Verhältnismässigkeit zu wahren“, abgelehnt (BWIS-II-Zusatzbotschaft, BBl 2010 5110).

#### **14. Oberaufsicht gegenüber dem BVGer (Art. 28)**

##### ***Problematik***

Entscheide des BVGer können von der parlamentarischen Oberaufsicht nicht überprüft werden. Die Arbeit der GPDel beschränkt sich somit auf die Kontrolle der grundsätzlichen Funktionsfähigkeit des Genehmigungsverfahrens. Dazu benötigt sie jedoch entsprechende Informationen des BVGer.

##### ***Antrag der GPDel***

Art. 28 Abs. 6 E-NDG (neu): *Der Präsident der zuständigen Abteilung des Bundesverwaltungsgerichts erstellt einen jährlichen Tätigkeitsbericht zuhanden der GPDel.*

##### ***Begründung***

Nach Art. 26 Abs. 4 ParlG ist die inhaltliche Kontrolle richterlicher Entscheide durch die Oberaufsicht ausgeschlossen. Ob genehmigungspflichtige Beschaffungsmassnahmen zu Recht bewilligt wurden, hat die GPDel somit nicht zu überprüfen.

Ihre umfassenden Informationsrechte ändern nichts daran, dass die GPDel auf die Fälle, die das BVGer bereits genehmigt hat, keinen korrigierenden Einfluss mehr ausüben kann. Es zeugt deshalb von einem unzureichendem Verständnis von der Arbeit der GPDel, wenn der Bundesrat die Einleitung seiner Erläuterungen zum 4. Abschnitt E-NDG, der die genehmigungspflichtigen Beschaffungsmassnahmen regelt, mit der vordergründig beruhigenden Versicherung abschliesst, dass die GPDel selbstverständlich vollen Zugang zu allen benötigten Daten und Akten haben werde (Botschaft NDG, S. 60).

Die GPDel könnte allenfalls beim NDB nachträglich kontrollieren, ob Massnahmen, die das BVGer bewilligt hat, nützliche Resultate geliefert haben. Würden sich die Fälle von nicht zweckmässigen Genehmigungen häufen, könnte die GPDel mit dem BVGer eine Aussprache darüber führen, um beurteilen zu können, ob allenfalls ein systematisches Problem vorliegt. Die Oberaufsicht könnte in der Folge versuchen, eine Verbesserung im Hinblick auf zukünftige Fälle zu bewirken.



Um die allgemeine Funktionsfähigkeit des Genehmigungsverfahrens kontrollieren zu können, wäre es nützlich, wenn die GPDel einmal pro Jahr mit dem BVGer eine Aussprache führen würde. Im Hinblick darauf sollte das Gesetz das BVGer beauftragen, jährlich einen Bericht über seine Tätigkeit in Erfüllung des Gesetzes zuhanden der GPDel zu verfassen.

## **15. Koordination zwischen dem E-NDG und der Revision des BÜPF**

### ***Problematik***

Während der Bundesrat offenbar die Absicht hegt, dem NDB alle Kompetenzen zu erteilen, welche die eidg. Räte im Rahmen der laufenden BÜPF-Revision den Strafverfolgungsbehörden gewähren werden, fehlen im E-NDG die notwendigen Koordinationsbestimmungen, um das E-NDG und das revidierte BÜPF entsprechend aufeinander abzustimmen.

### ***Empfehlung der GPDel***

Mit der Beratungen der Bestimmung des E-NDG, welche von der laufenden BÜPF-Revision betroffen sind, sollte erst nach Abschluss dieses Geschäftes in beiden Räten begonnen werden.

Die vorberatenden Kommissionen sollten zum geeigneten Zeitpunkt beim Bundesrat eine Zusatzbotschaft zu den NDG-spezifischen Änderungen im BÜPF einholen.

### ***Begründung***

Laut Art. 25 Abs. 1 Bst. a E-NDG soll der NDB alle Kompetenzen erhalten, welche der Strafverfolgung gestützt auf das heute geltende BÜPF zukommen. Die dafür notwendigen Anpassungen des heutigen BÜPF finden sich im Anhang betreffend die Änderung anderer Erlasse.

Offenbar ist es aber auch die Absicht des Bundesrats, dass pauschal alle Möglichkeiten, die mit der Totalrevision des BÜPF (13.025) von den eidg. Räten genehmigt werden, ebenfalls dem Nachrichtendienst zur Verfügung stehen sollen.

Die Vorlage enthält jedoch keine Bestimmungen, die eine Koordination mit der laufenden Totalrevision des BÜPF sichergestellt hätten. Einzig in den Erläuterungen werden verschiedene Bestimmungen angeführt, die zugunsten des NDB noch in das BÜPF eingefügt werden sollten (Botschaft NDG, S. 118ff). Die vorgeschlagene Übernahme von Formulierungen aus der Strafverfolgung erscheint jedoch nicht überall ausreichend durchdacht (z.B. Art. 22a BÜPF).

Offenbar geht der Bundesrat davon aus, dass zu gegebener Zeit das Parlament selbstständig dafür sorgen wird, dass das totalrevidierte BÜPF an die Bedürfnisse des NDB angepasst wird.

In den Erläuterungen wird ferner eine Bestimmung für den E-NDG vorgeschlagen, die den Einsatz von Überwachungsgeräte (IMSI-Catcher) erlaubt, welche auch Gegenstand der BÜPF-Totalrevision (Art. 269bis E-StPO) sind.

Den Einsatz von Trojanern durch den NDB ermöglicht hingegen Art. 25 Abs. 1 Bst. d Ziff. 1 E-NDG, indem er dem NDB erlaubt, in fremde Computersysteme (inkl. Laptops, Smartphones, etc.) einzudringen, um dort vorhandene oder übermittelte Informationen zu beschaffen. In den Erläuterungen wird dies jedoch weder explizit gesagt, noch ausgeführt, wie dies bewerkstelligt werden soll.



## 16. Eindringen in ein Computersystem zur Informationsbeschaffung (Art. 25 und 36)

### Problematik

Ob eine Genehmigungspflicht für das Eindringen in fremde Computersysteme besteht, hängt gemäss E-NDG vom Standort des betroffenen Systems und dem Ort ab, von welchem aus der NDB die entsprechende Massnahmen vornimmt. Dies schafft Unsicherheiten und relativiert die Rolle des BVGer gerade für jene Beschaffungsmassnahmen, die potentiell am weitesten in die Privatsphäre eindringen können. Das Eindringen in Computersysteme zur Informationsbeschaffung sollte deshalb in jedem Fall vom BVGer bewilligt werden müssen.

### Anträge der GPDel

Art. 36 Abs. Eindringen in Computersysteme und –netzwerke

2 Der NDB kann ~~zur Erfüllung seiner gesetzlichen Aufgaben auch von der Schweiz aus~~ in Computersysteme und Computernetzwerke im Ausland eindringen, um dort vorhandene oder von dort aus übermittelte Informationen über Vorgänge im Ausland zu beschaffen. ~~In politischen Fällen holt die Direktorin oder der Direktor des NDB die Zustimmung der Chefin oder des Chefs des VBS ein.~~

3 (neu) Das Genehmigungsverfahren richtet sich nach den Artikeln 28–31.

### Begründung

Art. 25 Abs. 1 Bst. d Ziff. 1 E-NDG erlaubt dem NDB, in fremde Computersysteme (inkl. Laptops, Smartphones, etc.) einzudringen, um dort vorhandene oder übermittelte Informationen zu beschaffen.

Damit kann der NDB einerseits Trojaner (vgl. Ziff. 15) einsetzen. Andererseits erhält der NDB auch die Kompetenz zum „Online-Durchsuchen“ eines Datenverarbeitungssystems, eine Möglichkeit, die auch mit der BÜPF-Totalrevision für die Strafverfolgungsbehörden nicht vorgesehen ist.

Während sich der Einsatz von Trojanern auf Informationen beschränkt, die vom betroffenen Eigentümer eines Computers an Dritte kommuniziert werden, erlaubt das Online-Durchsuchen den Zugang zu Informationen, die der Benutzer von sich aus mit niemanden zu teilen bereit ist. Der Eingriff in die Privatsphäre ist somit potentiell noch grösser, ebenso die Menge an Informationen, die von der Massnahmen betroffen sein kann.

Die Erläuterungen zu Art. 25 E-NDG erwecken den Eindruck, dass das Eindringen in ein fremdes Computersystem immer die Genehmigung des BVGer und des Vorstehers VBS benötigt. Dies ist allerdings nur der Fall, wenn sich das betroffene System in der Schweiz befindet. Dies ergibt sich *e contrario* aus Art. 36 Abs. 2 E-NDG, der die Informationsbeschaffung aus Computersystemen mit Standort im Ausland regelt und dafür explizit keine Genehmigung des BVGer verlangt.

Befindet sich der Computer im Ausland, so sieht Art. 36 Abs. 2 E-NDG lediglich bei „politisch heiklen Fällen“ eine Genehmigung durch den Chef VBS vor. Dies gilt allerdings nur, wenn der Ausgangspunkt für das Eindringen in der Schweiz und nicht im Ausland liegt.

Somit kann es gestützt auf Art. 36 Abs. 2 E-NDG erlaubt sein, ohne Genehmigung des BVGer in den Laptop oder das Smartphone einer Schweizer Person einzudringen.





Als Voraussetzung genügt es, dass sich die Schweizer Person mit ihrem Gerät im Ausland befindet und die Informationsbeschaffung einer Bedrohung gilt, die auch eine plausible transnationale Komponente hat, was beispielsweise beim internationalen Terrorismus der Fall ist. Aufgrund der weiten Verbreitung von mobilen Geräten und dem sehr aktiven Reiseverhalten von Schweizern ist dies nicht bloss ein hypothetisches Szenario.

Auch der Genehmigungsvorbehalt für die Auslandsbeschaffung im Inland (Art. 35 Abs. 2 E-NDG) ist wirkungslos für das Eindringen in mobile Geräte, wenn ihre Schweizer Besitzer mit ihnen ins Ausland reisen.

Es kann auch sein, dass ein Trojaner, der zur Beschaffung im Ausland eingesetzt wird, Daten an den NDB weitergibt, wenn die Person in die Schweiz reist. Ein solches Vorgehen müsste jedoch nach Art. 25 E-NDG vom BVGer genehmigt werden.

Die ursprüngliche BWIS-II-Vorlage von 2007 verlangte für das Eindringen in ein fremdes Computersystem noch eine gerichtliche Genehmigung unabhängig vom Standort des Gerätes (Art. 18m E-BWIS betreffend des geheimen Durchsuchens eines Datenverarbeitungssystems). D.h. die Genehmigungspflicht galt auch für den Fall, dass sich ein Computer im Ausland befand.

Das vom E-NDG vorgeschlagene Kriterium des Standortes des betroffenen Computersystems stellt die Wirksamkeit des vorgesehenen Genehmigungsverfahrens grundsätzlich in Frage. Dem BVGer kann keine Kontrollfunktion zukommen, da es von den potenziell problematischen Fällen gar nie erfährt. Es kann auch nicht Aufgabe der GPDel sein, alle Computersysteme, in welche der NDB ohne Genehmigung des BVGer eingedrungen ist, auf ihren jeweiligen Standort zu überprüfen.

Ein vertrauenswürdiges Kontrollkonzept setzt voraus, dass alle Massnahmen nach Art. 25 Abs. 1 Bst. d Ziff. 1 E-NDG und Art. 36 Abs. 2 E-NDG nach dem gleichen Verfahren genehmigt werden. Dieses soll unabhängig davon Geltung erhalten, wo sich das betroffene Computersystem befindet und von welchem Ausgangspunkt aus in dieses eingedrungen wird.

Für den Fall, dass die Massnahme ausschliesslich der Informationsbeschaffung über Vorgänge im Ausland dient, kann auf die Pflicht zur nachträglichen Mitteilung nach Art. 32 E-NDG verzichtet werden, wie dies der E-NDG auch für die Kabelaufklärung vorschlägt.

## **17. Sabotage von Computersystemen im Inland (Art. 25 und 28)**

### ***Problematik***

Nach Art 25 Abs. 1 Bst. d Ziff. 2 E-NDG soll der NDB die Kompetenz erhalten, mit elektronischen Massnahmen Computersysteme in der Schweiz daran zu hindern, kritische Infrastrukturen des Landes anzugreifen. Aus dieser Bestimmung erwächst jedoch ein Koordinationsbedarf, um zu verhindern, dass solche Massnahmen mit der Arbeit der Strafverfolgungsbehörden in Konflikt geraten.

### ***Antrag der GPDel***

Neuer Art. 28 Abs. 2bis E-NDG gemäss Antrag von Ziff. 13 (BVGer sorgt bei Bewilligung für den Vorrang der Strafverfolgung)



### **Begründung**

Werden Computersysteme und Computernetzwerke für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet, so kann der NDB dort eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen.

Befinden sich die fremden Computer im Inland, benötigt der NDB dafür laut Art 25 Abs. 1 Bst. d Ziff. 2 E-NDG eine Genehmigung des BVGer.

Die Erläuterungen äussern sich nicht weiter zu den Massnahmen, mit denen die Störung, Verhinderung oder Verlangsamung des Zugriffs auf Informationen bewerkstelligt werden soll. Mit dem genannten Zweck lässt sich allerdings jeder Eingriff begründen, der in irgendeiner Form den Datenfluss zwischen den Komponenten eines Computers oder mit anderen Systemen beeinträchtigt.

Die Möglichkeiten umfassen somit auch die Veränderung von Programmen, um interne Speicherzugriffe zu verändern, bis zur Überlastung der Internetverbindung des angegriffenen Computers durch eine zu grosse Anzahl von Verbindungsanfragen. Ausgeschlossen ist auch nicht, dass Daten gelöscht werden dürfen. Letzteres ist wohl das sicherste Mittel um den Zugriff auf Informationen in einem System zu verhindern.

Problematisch wäre insbesondere, wenn der NDB auf dem angegriffene Computer Daten löschen oder verändern würde, die später auch als Beweismaterial in einem Strafverfahren benötigt würden.

Laut den Erläuterungen darf der NDB nur eingreifen, falls die Computersysteme und Computernetzwerke für Angriffe auf kritische Infrastrukturen verwendet werden (Botschaft NDG, S. 59). Zweck der Massnahme sei es, die „Abwehr“ eines drohenden oder „während eines laufenden Angriffs ganz oder teilweise eingetretenen Schaden“ (Botschaft NDG, S. 62).

Falls der NDB die Vorbereitungen eines Angriffs entdeckt oder von einem laufenden Angriff erfährt, hat er somit die Kompetenz, mit geeigneten Mitteln die Computersysteme, die am Angriff beteiligt sind, an dessen weiteren Durchführung zu hindern. Der Polizei hingegen steht die Möglichkeit eines solchen elektronischen Eingreifens nicht offen. Erfährt sie von einem Computersystem, das für einen laufenden Angriff eingesetzt wird, kann sie jedoch vor Ort diesem Gerät einfach sozusagen „den Stecker rausziehen“.

Laut den Erläuterungen zu Art 25 Abs. 1 Bst. d Ziff. 2 E-NDG sollen allfällige Strafverfahren vorgehen und der NDB könnte nur tätig werden, wenn die Voraussetzungen für ein Strafverfahren (noch) nicht gegeben sind oder ein solches für die Abwehr eines tatsächlichen Angriffs aussichtslos ist (Subsidiaritätsprinzip). Sowohl der Gesetzesentwurf wie auch die Erläuterungen schweigen sich jedoch darüber aus, wie der NDB diesem Anspruch gerecht werden will.

Die Koordinationsbestimmung von Art. 28 Abs. 2bis E-NDG, die unter Ziff. 13 vorgeschlagen wird, kann allfällige Konflikte zwischen dem Vorgehen des Nachrichtendienstes und der Strafverfolgung entschärfen. Dies ist allerdings nur gewährleistet, wenn der NDB gegenüber dem BVGer das ordentliche Genehmigungsverfahren einhält und nicht das Dringlichkeitsverfahren nach Art. 30 E-NDG anwendet.



## **18. Sabotage von Computersystemen im Ausland (Art. 36)**

### ***Problematik***

Bei einem „Gegenangriff“ des NDB auf Computersysteme im Ausland, die ihrerseits für Angriffe auf die Schweiz benutzt werden, stellen sich verschiedene völkerrechtliche Fragen, die in der Botschaft nicht besprochen werden.

### ***Empfehlung der GPDeI***

Die eidg. Räte sollten abklären, ob eine rechtliche Präzisierung notwendig ist, unter welchen Umständen der Bundesrat den NDB gegen Computer im Ausland einsetzen kann und – mit Blick auf die bilateralen Beziehungen - welchen Schaden dabei in Kauf genommen werden kann.

### ***Begründung***

Art. 36 Abs. 1 E-NDG erlaubt einen „Gegenangriff“ auf Computersysteme im Ausland, die für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet werden.

In den Erläuterungen werden allenfalls relevante Fragen zur Koordination mit der Strafverfolgung und der Rechtshilfe nicht thematisiert. Was passiert beispielsweise, wenn die Schweiz bei einem Angriff von kriminellen Tätern aus dem Ausland dort um Rechtshilfe nachsucht und dieser Staat dann bemerkt, dass die involvierten Computer ihrerseits wieder von der Schweiz aus angegriffen wurden?

Bei einem elektronischen Angriff kann es äusserst schwierig sein, die Computer an der Quelle des Angriffs einwandfrei zu identifizieren. Aufgrund ungenügender Kenntnisse können die Massnahmen des NDB deshalb auch fremde Computer betreffen, die überhaupt nicht oder zumindest nicht mit Wissen ihres Eigentümers am Angriff auf die Schweiz teilgenommen haben. Aufgrund ungenügender Kenntnisse über den Angreifer oder technischer Vorgehensfehler können unbeabsichtigte Schäden im Ausland entstehen.

Die Erläuterungen schweigen sich über die völkerrechtlichen Implikationen aus, die der Bundesrat bei der Genehmigung nach Art. 36 Abs. 1 E-NDG zu berücksichtigen hat. Dazu haben das Bundesamt für Justiz (BJ) und die Völkerrechtsdirektion (DV) bereits zwei Gutachten erstellt:

- Gutachten des BJ und der DV über Rechtsgrundlagen für Computernetzwerkoperationen durch Dienststellen des VBS vom 10. März 2009 (publiziert in VPB 3/2009)
- Gutachten des BJ und der DV über Computer Network Operations (CNO) - Rechtliche Grundlagen und völkerrechtliche Aspekte von Gegenmassnahmen im Fall eines Cyber-Angriffs gegen die Schweiz, vom 1. November 2013 (nicht publiziert).

Kann ein Cyber-Angriff in einem konkreten Fall nicht einem Staat zugerechnet werden, so ist ein unilaterales Eingreifen gegen die betreffenden Computer völkerrechtlich unzulässig, da in diesem Fall die notwendige zwischenstaatliche Dimension fehlt.

Kann der Cyber-Angriff einem Staat zugerechnet werden, so ist völkerrechtlich zu unterscheiden, ob der Vorfall die Schwelle eines bewaffneten Angriffs im Sinne von Art. 51 der UNO-Charta erreicht. Die Schweiz würde sich dann im Kriegszustand mit dem Staat befinden, und vergleichbare Gegenmassnahmen wären völkerrechtlich zulässig. Liegt durch den Cyber-Angriff kein bewaffneter Angriff, sondern allein eine Verletzung des völkerrechtlichen Interventionsverbotes vor, schliesst das Völkerrecht unter bestimmten Voraussetzungen nicht



aus, dass die Schweiz unilateral vergleichbare Gegenmassnahmen im Cyber-Bereich ergreifen kann.

## **19. Kooperation mit Partnerdiensten in der Beschaffung (Art. 33 Abs. 1)**

### ***Empfehlung der GPDeI***

Zu prüfen ist, inwiefern der NDB Partnerdienste in die Durchführung von genehmigungspflichtigen Beschaffungsmassen einbeziehen darf.

### ***Begründung***

Nach Art. 33 Abs. 1 E-NDG kann der NDB mit ausländischen Nachrichtendiensten bei der Informationsbeschaffung in der Schweiz zusammenarbeiten.

Diese Möglichkeit besteht grundsätzlich auch bei genehmigungspflichtigen Massnahmen.

Die Bestimmung verlangt aber, dass ein beauftragter Partnerdienst Gewähr dafür bietet, dass die Schweizer Rechtsordnung eingehalten wird.

Gerade beim Einsatz von technischen Geräten oder Spionage-Software des Partnerdienstes in der Schweiz dürfte sich der NDB allerdings kaum sicher sein können, dass diese nicht noch anderen Zwecken als der vom NDB beabsichtigten Zusammenarbeit dienen. So könnte der NDB in einer gemeinsamen Operation mit einem Partnerdienst für diesen eine Spionage-Software auf den Computer einer Zielperson laden, um von den damit beschafften Informationen zu profitieren. Letztlich wäre aber wohl nur der Ersteller des Programms in der Lage zu entscheiden, welche Informationen auch beim NDB ankommen würden.

Aus den Erläuterungen geht nicht hervor, wie der NDB gegenüber dem BVGer belegen kann, dass sich der Partnerdienst an das Schweizer Recht halten wird.

Es stellt sich somit die grundsätzliche Frage, wie weit es vertretbar ist, dass der NDB insbesondere im Bereich der genehmigungspflichtigen Massnahmen technische und andere Formen der Unterstützung seitens ausländischer Dienste in Anspruch nimmt.

## **20. Kooperation mit Privaten in der Beschaffung (Abs. 33 Abs. 2)**

### ***Empfehlung der GPDeI***

Zu prüfen ist, ob der NDB Private mit der Durchführung von genehmigungspflichtigen Beschaffungsmassen beauftragen darf.

### ***Begründung***

Nach Art. 33 Abs. 2 E-NDG kann der NDB auch Private mit der Informationsbeschaffung beauftragen.

Laut den Erläuterungen kann es sich dabei um Beschaffungsmassnahmen handeln, die komplexe technische Überwachungsgeräte benötigen, welche nur von spezialisierten Privatfirmen betrieben werden. Denkbar sei auch der Einsatz von privaten Informatikspezialistinnen und Informatikspezialisten bei besonders geschützten Datennetzwerken (Botschaft NDG, S. 69). Restriktionen, beispielsweise gegenüber ausländischen Firmen, werden keine genannt.



Art. 33 Abs. 2 E-NDG erlaubt es letztlich, technische und personelle Kernkompetenzen, die der NDB benötigt, *extern einzukaufen*, um seine neuen Kompetenzen für die Informationsbeschaffung überhaupt zur Anwendung zu bringen. Die Möglichkeit des Beizugs von Externen birgt die Gefahr, dass das VBS keine hinreichende Klarheit über den effektiven Personalbedarf, welcher mit dem Ausbau der Kompetenzen des NDB verbunden ist, erlangt (vgl. Ziff. 30).

Laut den Erläuterungen soll mittels Vertrag gewährleistet werden, dass diese Externen das schweizerische Recht einhalten, besonders wenn sie für einen wesentlichen Teil der Vorbereitung und Durchführung der Beschaffungsmassnahme verantwortlich sind. Dies kann der NDB aber nur überprüfen, wenn er selber über die notwendigen Kernkompetenzen im Dienst verfügt, um beispielsweise das Funktionieren einer Spionage-Software zu verstehen.

Wenn externe Firmen für den NDB Informationen beschaffen, stellt sich auch die Frage, ob und wie die beschafften Daten dort bearbeitet werden und wer für den Datenschutz und die Aufsicht verantwortlich ist.

Nach den Erläuterungen würde es genügen, die Informationssicherheit und den Datenschutz im Vertrag mit den Externen zu regeln. Wie der NDB die Informationssicherheit und den Datenschutz bei den beigezogenen Externen überprüfen wird, lassen die Erläuterungen offen, ebenso wie die „Kontrollrechte des EDÖB“ ausgeübt werden sollen (Botschaft NDG, S. 69). Unklar ist auch, ob die ND-Aufsicht berechtigt wäre, die notwendigen Audits bei den externen Dienstleistern durchzuführen.

## **21. Quellenschutz gegenüber den Strafverfolgungsbehörden (Art. 34 Abs. 2 und 4)**

### ***Problematik***

Art. 34 Abs. 2 und 4 E-NDG entsprechen inhaltlich weitgehend dem heutigen Art. 17. Abs. 5 BWIS, der auf einen Mitbericht der GPDeI zur BWIS-II-Revision zurückgeht. Heute entscheidet im Streitfall das BStGer. Es gibt keinen Grund, diese von der GPDeI erarbeitete Lösung wieder in Frage zu stellen und dafür das BVGer zuständig zu machen.

### ***Antrag der GPDeI***

34 Abs. 4 E-NDG (Änderung): Im Streitfall entscheidet das ~~Bundesverwaltungsgericht nach Artikel 36a VG~~. *Bundesstrafgericht*. Im Übrigen gelten die massgebenden Bestimmungen über die Rechtshilfe.

### ***Empfehlung der GPDeI***

Zu prüfen wäre auch, ob aus Gründen der Verständlichkeit die Reihenfolge von Absatz 3 und 4 nicht vertauscht werden sollte.

### ***Begründung***

Aufgrund ihrer Abklärungen zum Fall des sogenannten „Rütli-Bombers“ war die GPDeI zum Schluss gelangt, dass unter bestimmten Umständen die Identität einer Inlandquelle schweizerischen Strafverfolgungsbehörden bekannt gegeben werden soll. Dies sollte namentlich dann erfolgen, wenn diese Person selbst einer von Amtes wegen zu verfolgenden Straftat verdächtigt wird oder die Bekanntgabe unerlässlich ist, um eine schwere Straftat aufzuklären.





Am 25. März 2011 machte die GPDel in ihrem Mitbericht einen entsprechenden Antrag, dem die eidg. Räte mit der Annahme des heutigen Art. 17 Abs. 5 BWIS folgten. Der Gesetzgeber entschied sich auch dafür, dass im Streitfall das BStGer entscheiden soll.

Art. 34 Abs. 2 E-NDG entspricht weitgehend der bisherigen Regelung im BWIS. Allerdings nimmt der Bundesrat in Absatz 4 einen Vorschlag, den das VBS bereits während der Beratung von BWIS-II-Zusatzbotschaft in der RK-S eingebracht hatte, wieder auf und sieht vor, dass im Streitfall nicht mehr das BStGer, sondern neu das BVGer zu entscheiden hat.

Der Bundesrat begründet dies vor allem damit, dass das BVGer mit dem E-NDG bereits als Genehmigungsinstanz eine wichtige Rolle erhält, und deshalb auch in Fällen der Rechtshilfe entscheiden soll.

Diese Argumentation übersieht jedoch, dass das BVGer keine Operationen mit menschlichen Quellen genehmigen muss und dass sich im Streitfall die anstehenden Rechtsfragen darauf konzentrieren, ob das aufzuklärende Delikt und eine allenfalls von der Quelle begangene Straftat die Preisgabe ihrer Identität an die Strafverfolgungsbehörden rechtfertigt.

## **22. Funkaufklärung und ihre Kontrollinstanz (Art. 37 und Art. 75)**

### **Problematik**

Die bisherige gesetzliche Regelung der Funkaufklärung und der Unabhängigen Kontrollinstanz (UKI), welche die Funkaufklärung auf ihre Rechtmässigkeit überprüft, gehen auf den Mitbericht zurück, welchen die GPDel im Jahr 2011 zur BWIS-II-Revision an die RK-S gerichtet hatte. Der E-NDG hat diese Bestimmungen (Art. 4a und 4b ZNDG) weitgehend in Art. 37 und Art. 75 E-NDG übernommen.

Aufgrund ihrer jährlichen Aussprachen mit der UKI konnte sich die GPDel ein Bild über die Praxis-tauglichkeit der von ihr veranlassten gesetzlichen Bestimmung machen. Aufgrund des erkannten Verbesserungsbedarfs beantragt die GPDel drei Modifikationen, die alle von der UKI unterstützt werden.

### **Antrag der GPDel zu Art. 37 E-NDG**

Art. 37 Abs. 6 E-NDG (Änderung): *Stösst er bei seiner Tätigkeit auf erfasste Kommunikationen, die keine Informationen über sicherheitspolitisch bedeutsame Vorgänge im Ausland und keine Hinweise auf eine konkrete Bedrohung der inneren Sicherheit enthalten, löscht er diese so rasch wie möglich.*

### **Begründung**

Die Bestimmung entspricht bis auf die Einleitung dem bisherigen Art. 4a Abs. 6 ZNDG. Die Änderung bewirkt eine Abgrenzung von Absatz 3, nach welchem der Bundesrat die Aufbewahrungsdauer regelt. Der ausführende Dienst muss eindeutig nicht verwendbare Kommunikationen nur dann vor Ablauf der Aufbewahrungsdauer löschen, wenn er solche im Rahmen seiner Arbeit bemerkt. Er muss folglich seine Daten nicht gezielt auf solche Kommunikationen absuchen, was bei der grossen Menge auch praktisch unmöglich wäre.

### **Anträge der GPDel zu Art. 75 E-NDG**

Art. 75 Abs. 1 E-NDG (Änderung): *Eine verwaltungsinterne, unabhängige Kontrollinstanz prüft die Funkaufklärung auf Rechtmässigkeit. Sie versieht ihre Aufgaben weisungsungebunden. Der Bundesrat wählt ihre Mitglieder.*



Art. 75 Abs. 2 E-NDG (Änderung): *Die Kontrollinstanz prüft die Aufträge an den durchführenden Dienst sowie die Bearbeitung und Weiterleitung der Informationen, die dieser erfasst hat. Sie erhält dazu von den zuständigen Stellen Zugang zu allen zweckdienlichen Informationen und Anlagen.*

### **Begründung**

Mit Art. 75 Abs. 1 E-NDG weicht der Bundesrat ohne Angabe von Gründen vom bisherigen Art. 4b Abs. 1 ZNDG ab und eröffnet bezüglich der Natur der UKI unnötigen Interpretationsspielraum.

Art. 75 Abs. 2 E-NDG entspricht der bisherigen Formulierung von Art. 4b Abs. 2 ZNDG. Diese Bestimmung hatte die UKI als problematisch erfahren, weil sie ihr letztlich vorschrieb, die Bearbeitung der erfassten Informationen vor und nach ihrer Weiterleitung vom durchführenden Dienst an den NDB zu überprüfen. Die UKI machte richtigerweise geltend, dass dies praktisch unmöglich sei. Die GPDel hatte mit der ursprünglichen Formulierung in erster Linie sicherstellen wollen, dass die Prüfung der UKI sowohl bei der Organisation, welche die Daten erfasst, als auch beim NDB erfolgen kann. Dies soll nun explizit so formuliert werden.

## **23. Kabelauflklärung (Art. 38 – 42)**

### **Problematik**

Wie aus den Erläuterungen zur Botschaft hervorgeht, sollen die vorgeschlagenen formell gesetzlichen Grundlagen für die Kabelauflklärung vorerst folgendem Zweck dienen:

- nähere technische Abklärungen und Versuche mit der Kabelauflklärung durchzuführen;
- eine Analyse der Datenströme durch die Schweiz vorzunehmen; und
- gestützt darauf abzuklären, ob mit der Kabelauflklärung auch in der Schweiz hinreichend nützliche Informationen gewonnen werden können.

Laut der Botschaft lässt sich der Aufwand für die Realisierung der Kabelauflklärung nicht abschätzen.

Ebenso grosse Unsicherheiten gibt es zum vorgeschlagenen Genehmigungsverfahren:

- Dem BVGer werden nur Kategorien von Suchbegriffen zur Genehmigung vorgelegt, weil viele der betroffenen Personen erst im Verlauf der Durchführung des Auftrags identifiziert werden können.
- Nach der Genehmigung müssen Suchbegriffe „dynamisch gehandhabt“ werden; eine Verfeinerung der Suchbegriffe ist erst im Verlauf der Aufklärungstätigkeit möglich.
- Die Genehmigung soll für 6 Monate erteilt werden, im Gegensatz zu den 3 Monaten für die Massnahmen nach Art. 25ff E-NDG.

Letztlich bedeutet dies, dass das BVGer jeweils eine sechsmonatige Machbarkeitsstudie genehmigen würde, welche zu einer „Suche im Heuhaufen“ ausufern könnte.

Unklar ist auch, wie das Gericht entscheiden soll, wie viele und welche Fernmeldedienstleister in die Erfüllung eines Aufklärungsauftrags einbezogen werden dürfen, damit eine Massnahme noch als verhältnismässig gelten kann.



### **Bemerkung der GPDel**

Die GPDel ist sich seit Jahren bewusst, dass ein wachsender Anteil der internationalen Kommunikationen über Kabel verläuft und die Funkaufklärung deshalb zunehmend an Bedeutung verliert. Es ist deshalb nachvollziehbar, wenn der Bundesrat den Nutzen der bisherigen Investitionen mit der Erschliessung neuer Datenquellen erhalten möchte.

Die GPDel ist aber nicht in der Lage zu beurteilen, ob das vom Bundesrat vorgeschlagene Vorgehen dieses Ziel letztlich auch erreichen kann.

## **24. Datenbanken und Qualitätskontrollen (Art. 43 – 56)**

### **Problematik**

Unter dem E-NDG ist eine Datenschutzkontrolle durch eine eigenständige Qualitätssicherungsstelle, wie sie das BWIS vorsieht, nur noch für 30 Prozent der bisherigen ISIS-Daten (d.h. die den gewalttätigen Extremismus betreffen) vorgesehen. Die Qualitätssicherung der restlichen ISIS-Daten und der Informationen aus der Auslandsbeschaffung, welche bisher im System ISAS bearbeitet wurden, wird hingegen den Benutzern dieser Daten überlassen, dies in Abweichung vom bisherigen Recht.

Abgelegt werden neue Daten dieser Art vorerst im sogenannten Restdatenspeicher gemäss Art. 56 E-NDG, der jedoch nur einer minimalen Qualitätskontrolle unterworfen ist. Eine wirksamere Qualitätskontrolle wird erst zwingend, wenn diese Daten in das System IASA NDB übernommen werden. Dies gilt jedoch nur für Meldungen, die vom NDB auch als ausreichend relevant beurteilt werden, um eine weitere Analyse zu rechtfertigen. Gleichzeitig lässt es der E-NDG explizit offen, ob bei einer Löschung von Daten in IASA NDB auch die entsprechenden Kopien im Restdatenspeicher zu löschen sind.

Damit der Restdatenspeicher nicht zu einer ausufernden Sammlung von wenig relevanten und kaum kontrollierten Daten anwächst, sollte zur Kompensation der schwachen Datenschutzregelung von Art. 56 E-NDG eine maximale Aufbewahrungsdauer ins Gesetz geschrieben werden. Damit würde auch der in der Botschaft nirgends angesprochene, aber zu erwartende Engpass bei den Personalressourcen für die Qualitätskontrollen etwas entschärft.

### **Antrag der GPDel**

Art. 56 Abs. 4 E-NDG (neu) *Die maximale Aufbewahrungsdauer der Daten beträgt 10 Jahre.*

### **Begründung**

#### **Bisherige Informationssysteme**

Nach dem bisherigen Recht werden alle Informationen, die nach BWIS beschafft wurden, im Staatsschutzinformationssystem (ISIS) bearbeitet. Das BWIS verlangt für die Daten in ISIS eine umfassende und regelmässige Datenschutzkontrolle sowie strenge Löschrufen.

Informationen aus der Beschaffung über das Ausland, werden teilweise im Informationssystem äussere Sicherheit (ISAS) bearbeitet. Mit der letzten ZNDG-Revision (13.064), die in der Frühjahrssession 2014 verabschiedet wurde, werden auch für die Daten in ISAS Erfassungskontrollen und periodische Qualitätskontrollen vorgeschrieben. Laut den Erläuterungen zu dieser Vorlage soll die interne Qualitätssicherungsstelle, die sich bei ISIS bewährt habe, auch diese Kontrollen übernehmen (Botschaft ZNDG vom 14.8.2013, BBl 2013 6673).



Weitere Informationen, die aus der Beschaffung über das Ausland stammen, finden sich in einem sogenannten Rohdatenspeicher (rund 4 Mio. Meldungen). Für dieses System existieren bisher keine Vorschriften für den Datenschutz.

Neben den Informationssystemen für nachrichtendienstliche Daten führte der NDB zudem verschiedene Systeme ein, in denen administrative und weniger sensitive Daten bearbeitet werden (GEVER NDB, OSINT-Portal, ELD, etc.) Die Fotopass-Daten werden als Folge einer Empfehlung des ISIS-Berichts der GPDel in einer eigenen Datenbank (P4, Quattro P) bearbeitet und müssen nach fünf Jahren gelöscht werden.

### Zukünftige Informationssysteme

Unter dem E-NDG wird das bisherige ISIS-System abgelöst.

Rund 30 Prozent der bisher in ISIS gespeicherten Meldungen (Stand 2013) werden in der neuen Datenbank IASA-GEX NDB gespeichert, die ausschliesslich Informationen zum gewalttätigen Extremismus enthalten soll. Die Daten in IASA-GEX NDB sollen weiterhin denselben Kontrollen unterstehen, die bisher für alle ISIS-Daten galten. Zuständig ist die dafür spezialisierte interne Qualitätssicherungsstelle.

Die übrigen 70 Prozent der ISIS-Daten und die Daten aus ISAS werden im zukünftigen System IASA NDB einem neuen Datenschutzregime unterstellt. Dort sind für die Qualitätssicherung die Benutzer des Informationssystems (d.h. die Mitarbeitende der Abteilung Auswertung) und nicht mehr – wie weiterhin in IASA-GEX NDB – die interne Qualitätssicherungsstelle, verantwortlich. Diese macht nur noch periodische Stichproben.

Allein um zu gewährleisten, dass es in IASA NDB zu keinen Abstrichen bei der Kontrolle der zuvor in ISIS bearbeiteten Daten kommt, müssten auf Seiten der Benutzer substantielle Personalressourcen für die Qualitätssicherung verfügbar gemacht werden.

In den Erläuterungen der Botschaft zum Personalbedarf finden sich allerdings keine Hinweise auf diese Problematik, weshalb ein Rückschritt hinter die Errungenschaften des BWIS unausweichlich scheint. Es muss auch erwähnt werden, dass die Abteilung Auswertung in den letzten Jahren nur unwesentlich von den zusätzlichen Ressourcen, die der NDB erhalten hat, profitiert hat.

Es besteht somit die Gefahr, dass die parlamentarische Oberaufsicht nach ein paar Jahren zu einem ähnlichen Befund wie bei ihrer ISIS-Inspektion kommen könnte, nämlich dass der NDB für IASA NDB nicht in der Lage war, die vorgeschriebenen Datenschutzkontrollen durchzuführen.

Während der E-NDG zwingend verlangt, dass Informationen über den gewalttätigen Extremismus ausschliesslich in IASA-GEX NDB bearbeitet werden müssen, können im Prinzip alle übrigen nachrichtendienstlich relevanten Informationen im sogenannten Restdatenspeicher nach Art. 56 E-NDB abgelegt werden. Die Informationen sollen gemäss den Erläuterungen aus der Funk- und Kabelaufklärung, von Partnerdiensten und von menschlichen Quellen stammen (Botschaft NDG, S. 88). Auch die Daten aus dem heutigen Rohdatenspeicher (s. oben) dürften dort Platz finden.

Ob im Restdatenspeicher abgelegte Meldungen auch in strukturierter Form in das System IASA NDB übertragen werden, entscheiden letztlich die Mitarbeitenden des NDB im Einzelfall. Sie entscheiden damit auch über die Intensität der Qualitätskontrolle für diese Informationen.

Anders als beispielsweise in IASA NDB erfolgt im Restdatenspeicher die periodische Überprüfung nämlich nicht anhand aller Informationen, die zu einer Person abgelegt sind



(Datensatz), sondern jeweils allein für eine eingegangene und im Restdatenspeicher abgelegte Meldung.

Die Wirksamkeit dieser Form von Qualitätssicherung beschränkt sich auf das Erkennen von Mängeln innerhalb einer einzigen Meldung. Eine Infragestellung der Richtigkeit oder Relevanz der Informationen in dieser Meldung durch andere Informationen erfolgt somit nicht. Allenfalls kann ein sachkundiger Benutzer bei der Kontrolle feststellen, dass eine Information nicht dem Stand seines persönlichen Wissens entspricht und abklären, ob deshalb die Information gelöscht werden soll.

Unterlässt es der NDB, eine Information aus dem Restdatenspeicher in das System IASA NDB zu übertragen, bleiben diese Daten allein diesem wenig wirksamen Datenschutzregime unterstellt.

Im Übrigen lässt das Gesetz offen, ob die Löschung einer registrierte Person und ihrer Daten in IASA NDB zur Folge hat, dass die Kopien dieser Daten auch im Restdatenspeicher gelöscht werden müssen. Art. 43 Abs. 3 E-NDG erlaubt nämlich explizit, dass Kopien derselben Daten in mehreren Systemen und dort nach unterschiedlichen Vorgaben bearbeitet werden.

Der Restdatenspeicher entpuppt sich somit entgegen seiner Bezeichnung als die Datenablage, in der sich im Vergleich zu den anderen Informationssystemen weitaus am meisten Daten ansammeln dürften und die jedoch gleichzeitig den schwächsten Qualitätskontrollen unterworfen ist.

Es stellt sich deshalb die Frage, ob die begrenzte Wirksamkeit der Qualitätskontrolle, wie sie aus Art. 56 Abs. 2 E-NDG hervorgeht, nicht durch eine Beschränkung der Aufbewahrungsdauer kompensiert werden sollte. Eine maximale Aufbewahrungsdauer von 10 Jahren erscheint zweckmässig, weil der NDB die ihn wirklich interessierenden Daten in der Zwischenzeit ja zwecks Analyse in das System IASA NDB übertragen kann. Gleichzeitig stellt die Reduktion der Datenmenge auch sicher, dass der Aufwand für die Qualitätskontrolle nicht explodiert.

## **25. Ungeklärte Kosten/Nutzen-Frage bei Quattro P / P4 (Art. 54)**

### ***Problematik***

Die GPDel betrachtet das aktuelle Fotopass-Programm, das die Daten für das System ‚Quattro P‘ liefert, bezüglich des Verhältnisses von Aufwand und Ertrag als ungenügend und hat (zusammen mit der FinDel) seine Abschaffung empfohlen. Eine Kann-Bestimmung würde es erlauben, die Weiterführung des Programms von seiner Effizienz abhängig zu machen.

### ***Antrag der GPDel***

Art. 54 Abs. 1 E-NDG (Änderung): Der NDB *kann* ein Informationssystem *betreiben*, das der Identifikation von bestimmten Kategorien von ausländischen Personen dient, die in die Schweiz einreisen oder aus der Schweiz ausreisen, und der Feststellung von deren Ein- und Ausreisedaten.

### ***Begründung***

Die Bestimmungen zum Informationssystem Quattro P entsprechen den bisherigen Vorgaben der Datenbank P4 zum Fotopassprogramm. Wird die Datenbank wie vom E-NDG vorgesehen im Gesetz festgeschrieben, erteilt der Gesetzgeber dem Bundesrat auch einen festen Auftrag, das Fotopassprogramm, das die GPDel ursprünglich zur Abschaffung empfohlen hatte, weiterzuführen (Jahresbericht der GPDel 2013, Ziff. 4.2.5, S. 70ff).





Falls die Weiterführung von Fotopass jedoch von seiner Effizienz abhängig gemacht werden soll, müsste Art. 54 E-NDG dieses System mit einer Kann-Bestimmung regeln.

## **26. Qualitätskontrollen bei Informationen aus beschaffungspflichtigen Massnahmen (Art. 46 und 57)**

### ***Problematik***

Genau für diejenigen Personendaten, die der NDB aufgrund der neuen Beschaffungsmittel nach Art. 25 E-NDG in dem ihm bisher nicht zugänglichen Bereich der Privatsphäre beschaffen darf, sieht der E-NDG keine Datenschutzkontrolle vor. Um diesen Mangel zu beheben, sollen diese Daten nicht mehr von den allgemeinen Vorschriften von Art. 46 E-NDG ausgenommen werden. Ausserdem sollen Daten, die nichts mit dem Ziel der genehmigten Beschaffungsmassnahme zu tun haben, rechtzeitig ausgeschieden werden (vgl. Antrag in Ziff. 13, der sich an der ursprünglichen BWIS-II-Vorlage von 2007 orientiert).

### ***Antrag***

Art. 46 Abs. 1 Bst. h. (neu) *Informationssystem für die Bearbeitung von Daten nach Artikel 57.*

Antrag aus Ziff. 13 zum neuen Art. 31a Abs. 1 E-NDG.

### ***Begründung***

Nach Art. 57 E-NDG werden die Daten aus der genehmigungspflichtigen Beschaffung (Art. 25 NDG) gesondert von den übrigen Informationssystemen bearbeitet. Dasselbe gilt auch für die Daten aus der Beschaffung über Vorgänge im Ausland, die mit den genehmigungspflichtigen Beschaffungsmassnahmen vergleichbar sind (Art. 35 Abs. 5 E-NDG).

Aus den Erläuterungen geht hervor, dass die beschafften Daten sehr umfangreich sein können und „viele Informationen enthalten, die nichts mit dem Aufklärungsziel zu tun haben, weil sie z.B. rein privater Natur sind“ (Botschaft NDG, S. 89). Dieser Hinweis dürfte vor allem die Daten betreffen, die über das Eindringen in fremde Computersysteme beschafft werden.

Auf das System nach Art. 57 E-NDG sind die allgemeinen Vorgaben, die aufgrund von Art. 46 E-NDG sonst für alle Informationssysteme des NDB gelten, nicht anwendbar. An ihrer Stelle tritt eine Sonderregelung nach Art. 57 Abs. 4 E-NDG. Der Bundesrat soll zwar die maximale Dauer für die Aufbewahrung der Daten festlegen (Art. 57 Abs. 4 Bst. c E-NDG), eine Qualitätskontrolle ist jedoch nicht vorgesehen.

Folglich sieht der E-NDG keine nennenswerte Datenschutzkontrolle genau für diejenigen Personendaten vor, die der NDB aufgrund der neuen Beschaffungsmittel nach Art. 25 E-NDG in dem ihm bisher nicht zugänglichen Bereich der Privatsphäre beschaffen darf.

Es ist somit notwendig, dass auch die Datenverarbeitung nach Art. 57 E-NDG unter die gleichen allgemeinen Regeln von Art. 44 und Art. 46 E-NDG fällt. Zu diesem Zweck ist das betreffende System in die Aufzählung der Informationssysteme nach Art. 46 Abs. 1 E-NDG aufzunehmen. Allenfalls könnte dies erlauben, Art. 57 Abs. 4 E-NDG zu streichen.

Ausserdem sollte die Aufbewahrungsdauer, insbesondere der grossen Masse von Daten, die nichts mit dem Aufklärungsziel zu tun haben, entsprechend beschränkt werden. Dazu dient auch der Antrag in Ziffer 13 des vorliegenden Dokuments, in Anlehnung an die BWIS-II-Vorlage von 2007, einen *neuen* Art. 31a Abs. 1 E-NDG einzuführen.



## **27. Weitergabe von Personendaten ans Ausland (Art. 60)**

### **Problematik**

Aus den Bestimmungen von Art. 60 E-NDG ist zu wenig klar erkenntlich, wie die Weitergabe von Personendaten ans Ausland in Abhängigkeit davon geregelt ist, ob der entsprechende Staat über eine mit der Schweiz vergleichbare Datenschutzgesetzgebung verfügt. Klarheit kann letztlich nur eine neue Systematik innerhalb des Artikels schaffen, wofür das BJ bereits in der Ämterkonsultation einen zweckmässig Vorschlag gemacht hatte.

### **Empfehlung der GPDeI**

Die vorberatende Kommission bittet das BJ um eine Neuformulierung von Art. 60 E-NDG. Als Ausgangspunkt für den Auftrag an das BJ schlägt die GPDeI folgende Bestimmungen vor:

#### **Art. 60 Weitergabe von Personendaten an ausländische Behörden**

<sup>1</sup> *Der NDB kann im Einzelfall Personendaten ins Ausland bekannt geben. Gewährleistet die Gesetzgebung des Empfängerstaates keinen angemessenen Datenschutz, so können Personendaten diesem Staat nur bekannt gegeben werden, wenn die Schweiz mit ihm diplomatische Beziehungen pflegt und eine der folgenden Voraussetzungen erfüllt ist:*

- a. *Die Schweiz ist aufgrund eines Gesetzes oder eines Staatsvertrags zur Bekanntgabe der Daten verpflichtet.*
- b. *Die Bekanntgabe ist im Einzelfall zur Wahrung eines überwiegenden öffentlichen Interesses unerlässlich.*
- c. *Die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität von Dritten zu schützen.*
- d. *Die betroffene Person hat eingewilligt oder die konkreten Umstände erlauben den Rückschluss auf eine solche Einwilligung.*
- e. *Der Empfängerstaat erbringt im Einzelfall hinreichende Garantien, die einen angemessenen Datenschutz gewährleisten.*

<sup>2</sup> *Er kann im Einzelfall Personendaten an Staaten weitergeben, mit denen die Schweiz diplomatische Beziehungen pflegt, wenn der ersuchende Staat schriftlich zusichert, über das Einverständnis der betroffenen Person zu verfügen, und dem ersuchenden Staat dadurch die Beurteilung ermöglicht wird, ob sie an klassifizierten Projekten des Auslandes im Bereich der inneren oder äusseren Sicherheit mitwirken oder Zugang zu klassifizierten Informationen, Materialien oder Anlagen des Auslandes erhalten kann. [wie Art. 17 Abs. 3 Bst. e LMSI]*

<sup>3</sup> *Personendaten dürfen einem Staat nicht bekannt gegeben werden, wenn die betroffene Person dadurch der Gefahr einer Doppelbestrafung oder ernsthafter Nachteile für Leib, Leben oder Freiheit im Sinne der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten oder anderer, von der Schweiz ratifizierter internationaler Abkommen ausgesetzt wird.*

<sup>4</sup> *Werden die Personendaten in einem Verfahren benötigt, so gelten die massgebenden Bestimmungen über die Rechtshilfe. [wie Art. 17 Abs. 5 BWIS]*

<sup>5</sup> *Der Bundesrat legt fest:*

- a. *die zugelassenen Empfänger;*
- b. *den Umfang der zu erbringenden Garantien.*



### **Begründung**

Art. 60 E-NDG entspricht abgesehen von redaktionellen Änderungen dem neuen Art. 6h ZNDG, der im Rahmen der letzten Revision dieses Gesetzes von den eidg. Räten in der Frühjahrssession 2014 angenommen wurde. Diese neuen Bestimmungen im ZNDG betreffen jedoch ausschliesslich Informationen, die aus der Beschaffung über das Ausland stammen. Im E-NDG sollen diese neuen Regeln auch für die Staatsschutzdaten aus dem Inland gelten, womit allerdings die bisherige Beschränkung der Weitergabe auf den Einzelfall dahinfällt.

Letztlich wirft jedoch Art. 60 E-NDG insbesondere auf die zukünftige Anwendung Fragen auf, die sich weder aus dem Wortlaut noch aus den Erläuterungen schlüssig beantworten lassen.

Ist Art. 60 Abs. 1 E-NDG nun der Regelfall und der NDB soll, wenn immer möglich, ausreichende Garantien zum Schutz der betroffenen Person einholen, damit die Weitergabe ans Ausland in Abweichung von den datenschutzrechtlichen Bestimmungen erfolgen kann? Betreffen diese Garantien die Person selbst oder nur ihre Daten?

Ist Art. 60 Abs. 1 E-NDG als *lex specialis* zu Art. 6 Abs. 2 DSG zu betrachten, dessen Ausnahmen laut der Botschaft zur Anwendung kommen müssen, wenn der ausländische Staat über keine mit der Schweiz vergleichbare Datenschutzgesetzgebung verfügt (Botschaft NDG, S. 90)? Kann sich der NDB somit nur auf die Garantien des Auslands stützen (analog zu Art. 6 Abs. 2 Bst. a DSG) und nicht auch auf die anderen Ausnahmen, die das DSG für die Datenweitergabe an Staaten ohne vergleichbare Datenschutzgesetzgebung vorsieht?

Setzt Art. 60 Abs. 2 E-NDG voraus, dass der ausländische Staat über eine vergleichbare Datenschutzgesetzgebung verfügt? Oder kommt dieser zweite Absatz immer dann zum Tragen, wenn der NDB vom ausländischen Staat die nach Absatz 1 vorgeschriebenen Garantien nicht erhalten kann?

Da Art. 60 Abs. 3 E-NDG in jedem Fall verlangt, dass eine Datenweitergabe ans Ausland unterbleiben muss, wenn die betroffene Person dadurch einer ernsthaften Gefährdung für Leib, Leben oder Freiheit ausgesetzt werden könnte, stellt sich ausserdem die Frage, ob der NDB unter solchen Umständen überhaupt berechtigt wäre, eine Garantie zum Schutz der betroffenen Person einzuholen.

Zu klären wäre ebenfalls, unter welchen Umständen ein Partnerdienst überhaupt den Schutz einer Person ausreichend garantieren kann, wenn sich die betroffene Person in der Schweiz oder in einem dritten Staat befindet.

Im Rahmen der Ämterkonsultation hatte das BJ dem NDB eine alternative Regelung für die Datenweitergabe ans Ausland vorgeschlagen, die in angepasster Form auf einfache Art und Weise die Unklarheiten des aktuellen Art. 60 E-NDG beheben könnte.

## **28. Auskunftsrecht (Art. 63)**

### **Problematik**

Nach der Absicht des Bundesrats sollten im E-NDG die Bestimmungen des bisherigen Art. 18 BWIS übernommen werden. Ein redaktioneller Fehler in Art. 63 Abs. 2 E-NDG führte jedoch dazu, dass sich der EDÖB für eine von zwei möglichen Antworten an den Gesuchsteller entscheiden muss, anstatt - wie nach bisherigem Recht - immer eine gleichlautende Antwort zu geben. Letzteres wird auch in Art. 65 Abs. 1 E-NDG explizit verlangt.

### **Antrag der GPDeI**

Art. 63 Abs. 2 E-NDG (Änderung) Er teilt ihr mit, *dass entweder in Bezug auf sie keine Daten unrechtmässig bearbeitet werden oder dass er im Falle von Fehlern bei der Datenbearbeitung*



*oder betreffend den Aufschub der Auskunft eine Empfehlung im Sinne von Artikel 27 DSG zu deren Behebung an den NDB gerichtet hat. [wie Art. 18 Abs. 4 BWIS]*

### **Bemerkungen**

Laut den Erläuterungen der Botschaft entspricht das Auskunftsrecht weitgehend der vom Parlament im Rahmen der BWIS-II-Zusatzbotschaft beschlossenen Lösung in Anlehnung an Art. 8 BPI (Bundesgesetz über die polizeilichen Informationssysteme des Bundes).

Während diese Aussage stimmt, erwähnen die Erläuterungen aber nicht, dass im Rahmen der letzten ZNDG-Revision für die Daten aus der Informationsbeschaffung über das Ausland mit Art. 6j ZNDG eine weniger restriktive Lösung nach Art. 8 und 9 DSG vorgeschlagen wurde, welche in der Frühjahressession auch von den eidg. Räten akzeptiert wurde. Auf Verordnungsstufe war diese Lösung bereits seit Anfang 2010 für das System ISAS in Kraft (Art. 23 ISV-NDB).

Somit vereinheitlicht der E-NDG das Auskunftsrecht im Sinne des restriktiveren Ansatzes der bisherigen gesetzlichen Lösungen.

Dies führt dazu, dass für mehr als die Hälfte der personenbezogen erfassten Daten des NDB das Auskunftsrecht im Vergleich zu den bisherigen rechtlichen Vorgaben eingeschränkt wird.

## **29. Archivierung (Art. 67)**

### **Problematik**

Die Vorlage erwähnt nirgends die neue Archivierungsregelung für den NDB, die aufgrund ihres letztjährigen Mitberichts der GPDeI an die SiK-S von beiden Räten im Rahmen der ZNDG-Revision zustande gekommen war. Ohne Begründung wird dem Parlament wieder eine neue Lösung vorgelegt. Der Vorschlag ist nicht nur unnötig, sondern auch nicht zweckmässig, weil er auf einem ungenügenden Verständnis des Archivierungsgesetzes beruht. Die eidg. Räte sollten deshalb für Art. 67 Abs. 2 E-NDG bei der Regelung bleiben, die sie vor kurzem in Art. 7a Abs. 2 ZNDG genehmigt haben.

### **Antrag der GPDeI**

*Art. 67 Abs. 2 E-NDG (Änderung) Für Archivgut, das von ausländischen Sicherheitsdiensten stammt, kann der Bundesrat gemäss Artikel 12 des Archivierungsgesetzes vom 26. Juni 1998 die Schutzfrist mehrmals befristet verlängern, wenn der betroffene ausländische Sicherheitsdienst Vorbehalte gegen eine allfällige Einsichtnahme geltend macht. [wie Art. 7a Abs. 2 ZNDG]*

### **Begründung**

In ihrem Mitbericht vom 9. Oktober 2013 zur ZNDG-Revision (13.064) hatte die GPDeI eine Lösung für die Archivierung der Unterlagen des NDB vorgeschlagen, die sich eng an den bestehenden Bestimmungen des Archivierungsgesetzes (BGA) orientierte. Für Unterlagen, die von ausländischen Diensten stammen, soll die Schutzfrist aber nicht nach einer einmaligen Dauer von 50 Jahre auslaufen, sondern der Bundesrat soll sie immer wieder verlängern können und dies solange wie der betroffene ausländische Partnerdienst auf einer Verlängerung besteht.



Der Antrag der GPDel wurde von beiden Räten in Art. 7a Abs. 1 und 2 ZNDG vollumfänglich übernommen. Das Parlament folgte dabei insbesondere auch nicht einem Gegenvorschlag, den das VBS in der erstberatenden Kommission (SiK-S) noch eingebracht hatte.

Der Ansatzpunkt für den besonderen Schutz der Unterlagen, die von ausländischen Diensten stammen, ist die Verlängerung der Schutzfrist, wie sie in Art. 12 Abs. 1 BGA vorgesehen ist.

Diese verlängerten Schutzfristen werden im Anhang 3 der Archivierungsverordnung (VBGA) ausgewiesen. Dies gilt beispielsweise für die Unterlagen aus den Mandaten, aufgrund derer die Schweiz fremde Interessen vertritt. Bekannte Fälle sind Iran und die USA oder Russland und Georgien.

In Art. 67 Abs. 2 E-NDG weicht der Bundesrat nun von dem von den eidg. Räten kürzlich gut geheissenen Ansatz ab. Anstatt sich auf die Verlängerung der Schutzfrist gemäss Art. 12 Abs. 1 BGA zu stützen, orientiert sich der neue Vorschlag des Bundesrats an Art. 12 Abs. 2 BGA. Der 2. Absatz von Art. 12 BGA lässt sich allerdings nur auf einzelne Aktenstücke anwenden und kann erst Geltung erlangen, nachdem ihre Schutzfrist bereits aufgehoben wurde. Der einzige Zweck von Art. 12 Abs. 2 BGA ist es, den Zugriff auf Akten nachträglich wieder einzuschränken, wenn irrtümlicherweise ihre Schutzfrist zu früh aufgehoben wurden. Diese Möglichkeit besteht bereits unter dem geltenden Archivierungsrecht.

Die Bestimmungen, welche die eidg. Räte auf Antrag der GPDel angenommen haben, verlangen hingegen, dass mit dem ausländischen Partnerdienst geprüft werden muss, ob die Schutzfrist für eine Kategorie von Akten wirklich aufgehoben werden kann, ohne dass befürchtet werden muss, dass nachträglich einzelne Akten daraus wieder dem Zugriff entzogen werden müssen.

### **30. Beobachtungsliste (Art. 71)**

#### ***Problematik***

Im Rahmen der BWIS-II-Revision übernahmen die eidg. Räten eine Regelung, wie der Bundesrat Organisationen, welche auf einer „Terror-Liste“ der EU oder der UNO figurieren, ohne weitere Abklärungen auch auf die Beobachtungsliste nehmen sollte.

Ein von der GPDel beim BJ in Auftrag gegebenes Gutachten zeigte aber, dass damit ein unerwünschter Automatismus zwischen diesen Listen und der Beobachtungsliste erzwungen wurde. Dieses Problem wurde leider im neuen Art. 71 E-NDG nur teilweise behoben.

#### ***Antrag der GPDel***

Es ist abzuklären, ob mit Art. 71 E-NDG effektiv bezweckt wird, dass eine Organisation, die nicht aufgrund tatsächlicher Gründe, sondern allein wegen ihrer Erwähnung auf einer internationalen Liste auf die Beobachtungsliste gesetzt wurde, dort solange nicht wieder gestrichen werden kann, wie sie auf einer internationalen Liste bleibt.

Falls Art. 71 E-NDG keine solche „Einbahnstrasse“ festschreibt, sondern dem Bundesrat den Spielraum einräumen soll, eine solche Organisation von der Beobachtungsliste zu entfernen, sollte Art. 71 E-NDG auch entsprechend formuliert werden.

#### ***Begründung***

Anlässlich der Behandlung der Zusatzbotschaft zur BWIS-II-Revision vom 27. Oktober 2010 wurden die Bestimmungen zur Beobachtungsliste (Art. 11 BWIS) angepasst. Obwohl dies vom NDB so nicht beabsichtigt worden war, stellte der neue Wortlaut einen Automatismus zwischen



den Organisationen auf den Terror-Listen der EU und der UNO und den Organisationen auf der Beobachtungsliste her. Entgegen der Ansicht des NDB war auch eine andere Auslegung nicht möglich, wie ein Gutachten des BJ vom 5. April 2013, welches die GPDel veranlasst hatte, ergab.

In ihrem Jahresbericht 2013 hatte die GPDel deshalb festgehalten, dass bei der Behandlung des E-NDG in den eidg. Räten das Verhältnis zwischen den internationalen Terrorlisten und der Schweizer Beobachtungsliste zu klären sei. Insbesondere sei diesmal sicherzustellen, dass die vom Parlament festgelegten Bestimmungen ohne Interpretationsspielraum auch der politisch gewünschten Intention entsprechen würden.

Nach Art. 71 Abs. 2 E-NDG genügt nun aber die Tatsache, dass eine Organisation beispielsweise auf der EU-Liste geführt wird, für die Annahme, die Organisation bedrohe die Sicherheit der Schweiz (gesetzliche Fiktion). In diesem Fall kann der Bundesrat eine solche Organisation – ohne weitere Begründung ihrer Gefährlichkeit – auf die Beobachtungsliste setzen. Er muss dies aber nicht tun. Bei der Aufnahme einer solchen Organisation besteht somit kein Automatismus zwischen den Listen.

Unklar ist jedoch, ob eine Organisation, die allein aufgrund der gesetzlichen Fiktion von Absatz 2 auf die Beobachtungsliste genommen wurde, später wieder von dieser gestrichen werden kann, falls sie weiterhin auf einer internationalen Liste, beispielsweise derjenigen der EU geführt wird.

Wenn keine tatsächlichen Anhaltspunkte dafür vorliegen, dass die Organisation die Sicherheit der Schweiz bedroht, müsste sie eigentlich nach Art. 71 Abs. 3 Bst. a E-NDG gestrichen werden können.

Weil aber die gesetzliche Fiktion von Absatz 2 die Annahme, dass die Organisation eine Bedrohung darstellt, solange aufrecht hält wie die Organisation auf der EU-Liste steht, ist es fraglich, ob Art. 71 Abs. 3 Bst. a E-NDG angewendet und damit die Organisation gestrichen werden kann.

Art. 71 Abs. 3 Bst. b E-NDG ist in diesem Fall nicht anwendbar, da er voraussetzt, dass die Organisation nicht mehr auf der betreffenden internationalen Liste steht. Einen Buchstaben c für eine Streichung in demjenigen Fall, dass die Organisation immer noch auf der internationalen Liste steht, findet sich in Art. 71 E-NDG hingegen nicht.

### **31. Personelle Auswirkungen (Ziff. 3.1.2 der Botschaft)**

#### ***Problematik***

Im Verlauf ihrer Inspektion zur Informatiksicherheit im NDB kam die GPDel zum Schluss, dass bei der Schaffung des NDB die Frage der notwendigen Personalressourcen zu wenig berücksichtigt worden war. Ebenso stellte die GPDel fest, dass im Vernehmlassungsbericht zum NDG nicht einmal die Hälfte des Personalbedarfs, welcher in der weniger ambitionierten BWIS-II-Vorlage von 2007 genannt war, ausgewiesen wurde. Um sicherzustellen, dass die bisher grösste Reform des Schweizer Nachrichtendienstes nicht aufgrund eines Missverhältnisses zwischen neuen Aufgaben und Ressourcen zum Scheitern verurteilt ist, verlangte die GPDel, dass der Bundesrat dem Parlament eine fundierte Analyse des Personalbedarfs präsentiert. Obwohl der Bundesrat mit seiner Botschaft zum NDG diese Empfehlung umzusetzen versprach, ist er diesem Auftrag der GPDel nicht nachgekommen.





### **Antrag der GPDeI**

Der Bundesrat soll in einer Zusatzbotschaft die von der GPDeI in ihrer Empfehlung 1 der Inspektion zur Informatiksicherheit im NDB verlangten Abklärungen nachholen. Allenfalls kann für die GPDeI und die FinDeI eine vertrauliche Aufstellung erstellt werden.

### **Begründung**

Aufgrund ihrer Inspektion zur Informatiksicherheit im NDB kam die GPDeI zum Schluss, dass bei der Zusammenlegung der zivilen Nachrichtendienste im VBS und der nachfolgenden Schaffung des NDB die Frage der notwendigen Personalressourcen ungenügend Gewicht erhalten hatte. Der Personalmangel in der Informatik hatte nach Meinung der GPDeI ein adäquates Risikomanagement des NDB verunmöglicht.

Die GPDeI war besorgt, dass mit der Umsetzung des E-NDB vergleichbare Herausforderungen auf den Nachrichtendienst zukommen würden wie bei der Schaffung des NDB. Die Delegation wollte deshalb verhindern, dass die damals gemachten Fehler wiederholt würden. Die GPDeI empfahl deshalb dem Bundesrat in der ersten Empfehlung ihres Inspektionsberichts, das VBS mit einer vertieften und detaillierten Analyse der personellen Ressourcen zu beauftragen, die für die Erfüllung der zusätzlichen Aufgaben, welche mit dem E-NDG vorgeschlagen werden, notwendig wären. Die Empfehlung erging am 2. Juli 2013 an den Bundesrat, d.h. nachdem der E-NDG in die Vernehmlassung gegangen war.

In der Botschaft an die eidg. Räte vom 19. Februar 2014 wird weder die Empfehlung 1 der GPDeI erwähnt noch findet sich in den Erläuterungen die gewünschte Analyse.

Die Ausführungen zu den personellen Auswirkungen (Ziff.3.1.2) unterscheiden sich so gut wie nicht von der Botschaft des Vernehmlassungsverfahrens. Die einzige Differenz ist, dass der Bundesrat den Personalbedarf neu mit 20.5 Stellen anstatt mit 16 Stellen veranschlagt. Zu bemerken ist allerdings, dass ein Teil des Personals für Stellen ausserhalb des NDB (BVGer, BAR, ZEO) geplant ist.

Unklar ist, ob die zwei neuen Stellen für NDB und ZEO, die in den Erläuterungen zu Art. 42 E-NDG erwähnt und für den Testbetrieb der Kabelaufklärung benötigt werden, zu dem ausgewiesenen Total von 20.5 Stellen gehören oder nicht.

Unklarheiten ergeben sich weiter zum Personalbedarf für die Qualitätssicherung der NDB-Daten. Einerseits sollen für die Qualitätssicherung insbesondere der neuen Informationssysteme zusätzliche Stellen geschaffen, andererseits sollen die gegenüber dem heutigen Stand steigenden Anforderungen an die Datenhaltung grösstenteils durch die vorhandenen Ressourcen aufgefangen werden (Botschaft NDG, S. 122).

Auch der Antrag des VBS an den Bundesrat vom 10. Februar 2014 enthält keine Analyse, die weiterführend ist als die Botschaft. Es wird einzig erwähnt, dass das EFD „mit den Details der Stellenberechnungen bedient“ worden sei.

Weder vom VBS noch vom Bundesrat hat die GPDeI weiterführende Informationen in Erfüllung der gemachten Empfehlung erhalten.

Angesichts der Tatsache, dass der Bundesrat im Jahr 2007 für die ursprüngliche BWIS-II-Vorlage 40 neue Stellen vorgesehen hatte, erscheint die heutige Einschätzung des Bundesrats von 20,5 als sehr problematisch.

Das NDG eröffnet nämlich neue Beschaffungsmittel nicht nur für den Inland-, sondern auch für den Auslandnachrichtendienst. Zweitens gehen die Informationsbeschaffungsmittel weiter als in der ursprünglichen BWIS-Vorlage. Drittens wird der Aufgabenbereich fest um den Schutz



kritischer Infrastrukturen und potentiell auf die Aussenpolitik und den Schutz des Werk-, Wirtschafts- und Finanzplatzes ausgedehnt.

Allein für letztere Aufgabe war das VBS im Jahr 2011 in einer Analyse auf einen Personalbedarf in der Beschaffung und Auswertung von rund 20 Vollzeitstellen gekommen.

Nach einer aktuellen Beurteilung würde zudem ein halbes Dutzend zusätzlicher Stellen nicht genügen, damit der NDB seinen aktuellen gesetzlichen Aufgaben im Bereich der Spionageabwehr nachkommen kann.