Informatiksicherheit im Nachrichtendienst des Bundes

Bericht der Geschäftsprüfungsdelegation der eidgenössischen Räte (Zusammenfassung) vom 30. August 2013

Stellungnahme des Bundesrates

vom 30. Oktober 2013

Bericht

1 Einleitung

1.1 Vorgeschichte

Der Nachrichtendienst des Bundes (NDB) existiert in seiner heutigen Form seit dem 1. Januar 2010. Vorher waren seine Aufgaben auf den Dienst für Analyse und Prävention (DAP, bis Ende 2008 im EJPD) und den Strategischen Nachrichtendienst (SND, VBS) aufgeteilt. Seine gesetzlichen Grundlagen findet der NDB insbesondere im Bundesgesetz vom 3. Oktober 2008 über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG, SR *121*) und im Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR *120*). Diese Rechtsgrundlagen sollen abgelöst werden durch ein neues Nachrichtendienstgesetz, das bis am 30. Juni 2013 in der Vernehmlassung war.

1.2 Synergien und Ressourcen

Bundesratsbeschluss vom 25. März 2009

Der Bundesrat hat am 25. März 2009 das VBS beauftragt, «die erforderlichen Massnahmen zu treffen, damit das ZNDG im Sinne der Zusammenführung der beiden Dienste DAP und SND in ein Bundesamt per 1. Januar 2010 umgesetzt werden kann». Im entsprechenden Aussprachepapier wurden auch die Auflagen für diese Umsetzung aufgeführt:

1. Umsetzung innert nützlicher Frist;
2. Umsetzung im Rahmen der bestehenden Gesetze;
3. Umsetzung ohne zusätzliche Ressourcen;
4. Transparenz und Kontrolle als permanente Aufgabe.

Bei der dritten Auflage wurde festgehalten: «Die angestrebte Lösung ist ohne zusätzliche Ressourcen zu realisieren.»

Parlamentarische Initiative Hofmann

Bereits die parlamentarische Initiative Hofmann vom 13. März 2007 (07.404: Übertragung der Aufgaben der zivilen Nachrichtendienste an ein Departement) hatte die Erhöhung der nachrichtendienstlichen Leistung zum Ziel:

«Es geht lediglich um die optimale Nutzung der vorhandenen nachrichtendienstlichen Informationen. Die Zusammenfassung der Aufgaben von DAP und SND unter einem Departement eröffnet zudem Möglichkeiten zur Nutzung von Synergien und zu einem effizienteren Einsatz der knappen Ressourcen.»

Entsprechend stand auch in der Stellungnahme des Bundesrates vom 23. April 2008 zum Bericht vom 29. Februar 2008 der Geschäftsprüfungskommission des Ständerates der optimierte Einsatz der vorhandenen Ressourcen im Zentrum (BBl *2008* 4038 f).

Die verschiedenen Vorstösse und Aussprachen, welche zur Schaffung des NDB führten, zeigen, dass vom neuen Dienst in erster Linie eine Mehrleistung im Kerngeschäft erwartet wurde.

Ausgangslage DAP und SND vor der Fusion zum NDB

Bei der Zusammenführung zweier Organisationseinheiten werden in der Regel Synergieeffekte durch das Wegfallen von Überlappungen in den Organisationen realisiert. Diesbezüglich war die Ausgangslage bei DAP und SND grundsätzlich eine andere.

Sowohl der DAP wie auch der SND verfügten nur sehr beschränkt bzw. überhaupt nicht über Querschnitts- und Supportfunktionen (Informatik, Dienste, Kommunikation, Personelles, Sicherheit, Recht und besondere Supportfunktionen im nachrichtendienstlichen Beschaffungsbereich). Der DAP bezog im EJPD beinahe sämtliche Leistungen über die zentralen Dienstleistungszentren des Departements und verfügte über keine eigenen Supportfunktionen. Der SND verfügte nur teilweise über ausreichende Supportfunktionen und bezog einen grossen Teil der Supportleistungen vom GS VBS. Der NDB musste nach der Fusion die benötigten Supportfunktionen selber sicherstellen und aus den bestehenden Ressourcen alimentieren. Hingegen ergab sich auf departementaler Ebene eine gewisse finanzielle Entlastung.

Der NDB in der Umsetzungsplanung zur Aufgabenüberprüfung (AÜP)

Der Bundesrat legte am 14. April 2010 in seinem Bericht zur Umsetzungsplanung zur Aufgabenüberprüfung (AÜP) für die 25 längerfristigen Massnahmen, die von den Departementen weiterverfolgt werden, Meilensteine fest. Diese Meilensteine wurden am 1. September 2010 bei der Verabschiedung der Botschaft zum Konsolidierungsprogramm 2012–2013 aktualisiert. Massnahme Nr. 13 betraf die «Erschliessung von Synergiepotenzialen bei den zivilen Nachrichtendiensten», wonach der Bundesrat 2011 über die Höhe und Verwendung des Synergiepotenzials zu beschliessen hat: «Daraus [aus der Zusammenführung] resultieren Synergiegewinne, die noch abschliessend zu quantifizieren sind und zugunsten des Bundeshaushalts abzuschöpfen sind.»

In einem vertraulichen Bericht vom 27. Mai 2011 zeigte das VBS dem Bundesrat auf, dass die Fusion von DAP und SND zum NDB durchaus Synergien erschlossen und zu internen Einsparungen geführt hatte. Dem standen jedoch neue, nicht finanzierte Aufgaben gegenüber, welche der NDB mit den realisierten Einsparungen finanzieren musste. Unter dem Strich resultierten für den Bund keine Einsparungen, dafür aber die verlangte Erhöhung der nachrichtendienstlichen Leistung.

Mit der Gutheissung dieses Berichts am 10. Juni 2011 entliess der Bundesrat den NDB aus der AÜP.

Die Informatik des NDB setzte seit dem Zeitpunkt der Fusion notwendigerweise auf die Aufrechterhaltung des Betriebs einer stark gewachsenen Anwendungs- und Infrastrukturlandschaft. Zur Sicherstellung dieses Betriebs mussten punktuell Lieferantenfirmen und externe Mitarbeitende eingesetzt werden. Im ob genannten Bericht war dem Bundesrat auch aufgezeigt worden, wie die seit 2010 erzielten Synergien zum Aufbau der verschiedenen Querschnittsfunktionen eingesetzt werden.

1.3 Erfüllte Zielsetzungen des Bundesrates

Der Bundesrat hat die Entstehung des NDB eng mit seinen jährlichen Zielsetzungen und der Berichterstattung begleitet.

2010: Schaffung der organisatorischen Grundlagen

2010 konnte der Aufbau des NDB überwiegend abgeschlossen werden. Das Prozessmodell NDB, die Prozesslandschaft sowie die Pilot-Prozesse für den Aufbau eines Geschäftsverwaltungssystems wurden definiert und dokumentiert. Die Normprozesse wurden gemäss Planung dokumentiert und umgesetzt. 2010 hat der Bundesrat auch über das weitere Vorgehen bezüglich der Gesetzgebung für den NDB entschieden. Am 27. Oktober 2010 verabschiedete er die Zusatzbotschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS II reduziert). Am 24. August 2010 genehmigte der Chef VBS den Projektantrag und das Konzept für den Entwurf eines neuen Nachrichtendienstgesetzes (ND-Gesetz); der Bundesrat hatte den Auftrag dazu am 27. November 2009 erteilt.

2011: Priorisierung der Arbeitsthemen und Qualitätssicherung

2011 standen die Priorisierung der Themenbereiche des neuen Grundauftrages des NDB, die Anpassung der rechtlichen Grundlagen und die Umsetzung der Empfehlungen der GPDel zur Qualitätssicherung des Informationssystems Innere Sicherheit (ISIS) im Vordergrund. Die Priorisierung der Themen wurde mit dem neuen Grundauftrag des Bundesrates anfangs 2011 abgeschlossen, die Umsetzung der Massnahmen sowie der Abbau der Pendenzen im ISIS erfolgten planmässig und für das ND-Gesetz wurde das Normkonzept erstellt.

2012: Abschluss Umsetzung Massnahmen ISIS-Bericht der GPDel – Cyberstrategie

2012 konnten die notwendigen Massnahmen (Anpassungen von Verordnungen, Weisungen und Organisationsvorschriften) für die Umsetzung von BWIS II mit der Inkraftsetzung per 16. Juli 2012 realisiert werden. Die empfohlenen Massnahmen des ISIS-Berichtes der GPDel konnten vollständig umgesetzt werden. Wesentlichen Anteil hatte der NDB auch an der Realisierung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken, die vom Bundesrat am 27. Juni 2012 gutgeheissen worden ist.

2013: Botschaft neues ND-Gesetz

2013 steht für den NDB wiederum die Rechtsetzung im Vordergrund: Es geht um die Verabschiedung der Botschaft zum neuen NDG (Vernehmlassung bis Ende Juni 2013) und die Verabschiedung der Botschaft zur Teilrevision des ZNDG. Letzteres Ziel hat der Bundesrat mit seinem Beschluss vom 14. August 2013 realisiert. Damit will er dem NDB ermöglichen, die auf sicherheitspolitisch bedeutsame Informationen aus dem Ausland anwendbare Datenbank ISAS auch nach Juni 2015 weiter zu betreiben, wenn bis dahin das neue NDG noch nicht in Kraft getreten sein sollte.

1.4 Erledigung von Pendenzen der Vorgängerorganisationen

Der Aufbau des NDB war von Beginn auch damit befasst, verschiedene Pendenzen seiner Vorgängerorganisationen abzubauen.

Revision des BWIS

Die Revision des BWIS («BWIS II reduziert»), für die der Bundesrat am 27. Oktober 2010 eine Zusatzbotschaft verabschiedet hatte, konnte mit der parlamentarischen Schlussabstimmung vom 23. Dezember 2011 nach rund einem Jahrzehnt Arbeit zu einem erfolgreichen Abschluss gebracht werden.

Pendenzen bei der Datenbearbeitung im ISIS

Dringender Handlungsbedarf zeigte sich unmittelbar nach der Schaffung des NDB hinsichtlich der Rückstände der Qualitätssicherung bei der Datenbearbeitung im ISIS. Am 21. Juni 2010 veröffentlichte die GPDel dazu einen Inspektionsbericht. Der Bundesrat nahm in seiner Stellungnahme vom 20. Oktober 2010 alle Empfehlungen grundsätzlich an. Um die Situation so rasch als möglich zu bereinigen, leitete der NDB die notwendigen Massnahmen in die Wege. Der Bundesrat konnte in seinem Geschäftsbericht 2012 feststellen, dass die im GPDel-Bericht erwähnten Datensätze, die einer ordentlichen Gesamtüberprüfung unterzogen werden mussten, per 5. Dezember 2012 vollständig bereinigt werden konnten. Der vom VBS eingesetzte externe Datenschutzbeauftragte, alt Ständerat Dr. Hansruedi Stadler, bestätigte den vollständigen Abbau der Pendenzen bei der Erfassungskontrolle und der Gesamtüberprüfung.

1.5 Lagebedingte Herausforderungen an den NDB

Seit 2010 stellen sich dem NDB, dem zusammengeführten Ausland- und Inlandnachrichtendienst, bedingt durch die Lageentwicklung verschiedene Herausforderungen:

Verschiebung der Beschaffungs- und Auswerteschwerpunkte

Obwohl die Schweiz nicht ein erklärtes prioritäres Ziel für dschihadistisch motivierte Anschläge ist, wurden in den vergangenen drei Jahren mehrere Schweizer Bürgerinnen und Bürger im Ausland Opfer von politisch oder terroristisch motivierten Entführungen. Infolge der gewalttätigen politischen Umwälzungen in den arabischen und nordafrikanischen Ländern musste eine Zunahme von dschihadistisch motivierten Reisebewegungen nicht nur in Europa, sondern auch aus der Schweiz festgestellt werden.

Akzentuiert durch die Lageentwicklung im Mittleren Osten, ist die Schweiz in den letzten drei Jahren vermehrt von intensiven Bestrebungen einzelner Länder betroffen, unter Umgehung von Gesetzen Dual-use-Güter zu beschaffen, um sie zur Entwicklung und Herstellung von Massenvernichtungswaffen und deren Trägersystemen zu verwenden. In den Vordergrund rückte auch die Aufdeckung und Abwehr von Angriffen auf kritische Informatikinfrastrukturen. Aktivitäten zur Ausforschung

von sich in der Schweiz aufhaltenden Regimegegnern und Oppositionellen durch ausländische Nachrichtendienste sowie zur illegalen Informationsbeschaffung auf dem Forschungs-, Werk-, Finanz- und Handelsplatz Schweiz waren vermehrt zu erkennen, wobei ein Trend hin zu Informatikangriffen feststellbar ist.

Anpassung der Fähigkeiten

Der Bundesrat nimmt zur Kenntnis, dass der NDB verschiedene Massnahmen ergriffen hat, um diesen neuen Herausforderungen zu begegnen, die sich aus der Lageveränderung ergeben haben:

- Seit 2010 passt der NDB zusammen mit den Kantonen laufend sein Präventionsprogramm PROPHYLAX zur Sensibilisierung für die Bedrohung durch Proliferation und Wirtschaftsspionage an. Angesprochen werden potenziell betroffene Unternehmen sowie Forschungs- und Bildungseinrichtungen. In diesem Programm sind insgesamt über 1800 Firmen und 100 Forschungsinstitutionen in der Schweiz und im Fürstentum Liechtenstein von Interesse. Ende September 2013 wurde die 1000. Firma kontaktiert.
- Seit 2011 führt der NDB zusammen mit der Bundeskriminalpolizei ein Dschihadismus-Monitoring durch. Der Bundesrat hat den NDB gestützt auf die Umsetzung der Motion 07.3751 Büchler mit Beschluss vom 10. Juni 2010 beauftragt, die Beobachtung von dschihadistischen Webseiten zu gewährleisten.
- 2012 hat der NDB im Bereich Gewaltextremismus mit der gemeinsamen Lagedarstellung erstmals eine aktuelle nationale Lageübersicht elektronisch bereitgestellt und damit die Grundlage für eine laufend aktuelle Lagebeurteilung geschaffen. Nach der Einführung der entsprechenden Rechtsgrundlage im BWIS konnte damit ein langjähriges Bedürfnis der Kantone erfüllt werden.
- Der NDB war 2012 mit der nachrichtendienstlichen Einheit der Melde- und Analysestelle Informationssicherung MELANI bei der Erarbeitung einer nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken durch das VBS beteiligt. Am 27. Juni 2012 hiess der Bundesrat ein entsprechendes Grundlagenpapier gut. Damit konnte mehreren parlamentarischen Vorstössen entsprochen werden.
- Am 1. Mai 2013 hat der Bundesrat die Aufgaben, Kompetenzen und Verantwortlichkeiten der bei der Lösung von Entführungsfällen beteiligten Dienststellen von EDA, EJPD und VBS genehmigt. Dem NDB fällt hier die Aufgabe der Lageverfolgung und Lagefortschreibung, Auswertung und Lagedarstellung sowie die Erbringung von operativen Dienstleistungen zu.

Gezielte Zusammenarbeit mit Partnern im In- und Ausland

Der NDB hat in den ersten drei Jahren die Zusammenarbeit mit den in- und ausländischen Partnern etabliert und gezielt ausgebaut.

Im Inland sind dies vor allem die Kantone und auf Bundesebene die in der Kerngruppe Sicherheit vertretenen Bundesstellen. Neue Akzente in der Zusammenarbeit mit den Kantonen ergaben sich durch neue Ausbildungsprogramme, die Anforde-

rungen der Qualitätssicherung sowie durch die Neuregelung der Aufsicht der Staatsschutzorgane in den Kantonen.

Bei der Zusammenarbeit mit ausländischen Diensten hat der fusionierte Dienst die Aufmerksamkeit auf diejenigen Partner gerichtet, die Aufgaben im Sinne des BWIS und / oder des ZNDG erfüllen. Der NDB verfolgt eine Partnerdienstpolitik, die dem Bundesrat jährlich zur Genehmigung vorgelegt wird.

2 Seit dem Vorfall getroffene Massnahmen des Bundesrates

2.1 Überprüfungen und Berichterstattung durch den C VBS

Am 22. April 2013 hat das VBS dem Bundesrat einen Bericht zur Kenntnis gebracht, der die Ereignisse rund um den verhinderten Datenabfluss und die daraufhin eingeleiteten bzw. noch einzuleitenden Massnahmen darstellt. Der Bericht stellt fest, dass keine Daten des NDB in unbefugte Hände gelangt sind. Ohne rasches und konsequentes Handeln innerhalb und ausserhalb der Verwaltung wäre es jedoch möglich gewesen, dass nachrichtendienstliche Daten an Dritte im In- und Ausland oder an die Öffentlichkeit hätten gelangen können.

Weiter führt der Bericht aus, wie VBS und NDB im Anschluss an die Ereignisse die notwendigen Führungsentscheide getroffen haben. Mehrere verwaltungsinterne und -externe Dienststellen und Expertengruppen wurden mit der Analyse der Situation und mit dem Aufzeigen des Handlungsbedarfs beauftragt. In eigener Kompetenz hat der NDB rund 40 Massnahmen identifiziert und eingeleitet. Es handelt sich dabei um technische und organisatorische Massnahmen sowie um die Einschränkungen von Zugriffen und Zutritten.

Der VBS-Bericht wurde im Anschluss an die Kenntnisnahme durch den Bundesrat der GPDel zugeleitet und am 30. April 2013 vom VBS veröffentlicht.

2.2 Erhöhung der personellen Ressourcen im Bereich Informatik und Sicherheit

Gleichzeitig mit der oben genannten Berichterstattung hat das VBS mit Antrag vom 26. April 2013 dem Bundesrat die Erhöhung der personellen Ressourcen in den Bereichen Informatik und Sicherheit des NDB beantragt.

Der Bundesrat hat mit Beschluss vom 1. Mai 2013 zur Kenntnis genommen, dass die notwendige und signifikante Erhöhung der Sicherheit und Informatiksicherheit beim NDB ab 2014 zu einem jährlichen Mehrbedarf von acht und ab 2015 von weiteren drei Stellen führen wird. Der Bundesrat hat anlässlich der Gesamtbeurteilung der Ressourcen im Personalbereich 2013 mit Beschluss vom 26. Juni 2013 gestützt auf diesen Antrag dem VBS acht Stellen ab dem Jahr 2014 zugesprochen. Das VBS hat dem NDB bereits in der ersten Hälfte des Jahres 2013 aus der Departementsreserve die umgehende Finanzierung dieser acht Stellen bewilligt.

Mit den zusätzlichen Stellen können sicherheitskritische Leistungen weitestgehend durch interne Mitarbeitende erbracht und aufgestaute Migrationsprojekte realisiert

werden. In der Informatik- und Betriebssicherheit können fehlende Fähigkeiten aufgebaut und Redundanzen geschaffen werden. Das Vier-Augen-Prinzip wird so insbesondere in besonders kritischen Aktivitäten während den erweiterten Betriebszeiten gewährleistet.

2.3 Informations- und Schulungsmassnahmen für das Bundeskader durch das EFD

Der Bundesrat hat als Folge des Datendiebstahls dem EFD am 15. März 2013 den Auftrag erteilt, Informations- und Schulungsmassnahmen für das Bundeskader in den Belangen der Informationssicherheit durchzuführen. Weitere Verbesserungen bei der Sicherheit werden sich als Folge eines neuen Informationssicherheitsgesetzes (ISG) ergeben, das unter der Führung des VBS erarbeitet wird. Zurzeit ist geplant, die Vernehmlassung zum ISG im Januar 2014 zu eröffnen.

Der Bundesrat anerkennt so den Handlungsbedarf, wie er in den Empfehlungen der GPDel formuliert ist, insbesondere die Massnahmen zur Informatiksicherheit und zum Risikomanagement. Er hat mit den Beschlüssen zur Aufstockung der Ressourcen in den Bereichen Informatik und Sicherheit auch die notwendigen Schritte zur Erhöhung der Sicherheit des Nachrichtendienstes unternommen.

3 Zu den Empfehlungen der GPDel

Zu den einzelnen Empfehlungen nimmt der Bundesrat wie folgt Stellung:

Empfehlung 1

Die GPDel empfiehlt dem Bundesrat, das VBS mit einer vertieften und detaillierten Analyse der personellen Ressourcen zu beauftragen, die für die Erfüllung der zusätzlichen Aufgaben, welche mit dem neuen ND-Gesetz vorgeschlagen werden, notwendig sind.

Der Bundesrat wird in seiner Botschaft zum neuen ND-Gesetz die finanziellen und personellen Auswirkungen der einzelnen neuen Massnahmen ausweisen. Die nach dem Datendiebstahl erkannten Mängel in der Informatik-Sicherheit sollen durch die am 1. Mai 2013 beschlossenen Massnahmen behoben werden. Der NDB wird aber auch mit dem neuen ND-Gesetz über – im internationalen Vergleich – sehr knappe Ressourcen verfügen und Schwerpunkte setzen müssen.

Empfehlung 2

Die GPDel ersucht den Bundesrat sicherzustellen, dass das VBS ihm bis Juni 2014 über den Stand des Risikomanagements im NDB Bericht erstattet und darlegt, wie der NDB die einschlägigen Vorgaben des Bundes zum Risikomanagement adäquat umsetzt.

Der Bundesrat folgt dieser Empfehlung, die Umsetzung ist bereits im Gange. Der Chef VBS hat am 9. Januar 2013 die Nachrichtendienstliche Aufsicht damit beauftragt, den weiteren Aufbau des Risikomanagements des NDB und die entsprechenden Massnahmen kontinuierlich zu beurteilen. Der Bundesrat kann auf dieser Grundlage sicherstellen, dass der NDB diese Vorgaben adäquat umsetzt.

Empfehlung 3

Die GPDel ersucht das VBS, dafür zu sorgen, dass der Informatiksicherheitsbeauftragte des Departements (ISBD VBS) auf Ende 2014 alle Anwendungen und Systeme des NDB darauf hin prüft, ob sie durch ein gültiges Sicherheitskonzept mit einer fundierten und umfassenden Risikobeurteilung abgedeckt sind. Die Behebung allfälliger Mängel ist mittels eines verbindlichen Massnahmenplans auszuweisen.

Der Bundesrat teilt die Meinung der GPDel, dass die Anwendungen und Systeme des NDB durch ein gültiges Sicherheitskonzept mit einer fundierten und umfassenden Risikobeurteilung abgedeckt sein müssen. Eine vollständige Inventur der Schutzobjekte ist erfolgt. Gestützt darauf wird nun durch den NDB, in Abstimmung mit dem ISBD VBS, ein Massnahmenplan (je Schutzobjekt), erstellt werden. Entsprechend folgt der Bundesrat dieser Empfehlung.

Empfehlung 4

Die GPDel ersucht den Bundesrat, beim VBS bis Ende 2013 überprüfen zu lassen, ob die Bestimmung von Art. 7 Abs. 1 ISV-NDB über die Chiffrierung des SiLAN so angewendet werden kann, dass der Aufwand und Nutzen für die Informatiksicherheit des NDB in einem vertretbaren Verhältnis stehen. Je nach Ergebnis der Überprüfung ist die Bestimmung entweder innert nützlicher Frist anzuwenden oder umgehend zu streichen.

Der Bundesrat nimmt diese Empfehlung zur Prüfung der Chiffrierung des SiLAN entgegen. Die in Art. 7 Abs. 1 ISV-NDB gemachte Aussage über die Chiffrierung des SiLAN beruhte auf einem legislatorischen Versehen, welches bei der Ausarbeitung der Verordnung nicht bemerkt wurde. Dennoch hat der NDB nach dem Datendiebstahl die Chiffrierung des SiLAN als wünschbare Massnahme zur Erhöhung der Informatiksicherheit aufgenommen. Bei der Planung der Umsetzung zeigte sich, dass der zusätzliche Nutzen der Chiffrierung in keinem vertretbaren Verhältnis zum Aufwand und den Risiken für die Informatiksicherheit steht, da eine Vollchiffrierung eine massive technische Leistungserhöhung – verbunden mit den entsprechenden Kosten – erfordern würde. Daraufhin wurde diese Massnahme verworfen. Der NDB hat im August/September 2013 die Ämterkonsultation zur geplanten Änderung der ISV-NDB durchgeführt. Dabei wird das SiLAN korrekterweise als autonome, geschützte Plattform beschrieben, die auf den Übertragungswegen teilchiffriert ist. Es ist möglich, dass mit fortschreitender technischer Entwicklung eine Vollchiffrierung künftig realistisch werden könnte.

Empfehlung 5

Die GPDel empfiehlt dem Bundesrat, mit einer Revision der PSPV dafür zu sorgen, dass für externe Mitarbeitende die gleichen Anforderungen an die Stufe PSP gestellt werden wie für Angestellte des Bundes, welche die gleichen Aufgaben wahrnehmen. Die Verantwortung für die Einhaltung der Vorschriften durch externe Firmen und ihre Mitarbeitenden ist derjenigen Bundesstelle zu übertragen, für welche die Externen letztlich ihre Leistungen erbringen.

Die heutige PSPV wird dem Anspruch bereits gerecht, dass für externe Mitarbeitende (Dritte) die gleichen Anforderungen an die Stufe der PSP gestellt werden, wie für Angestellte des Bundes, welche die gleichen Aufgaben wahrnehmen. So kann für Dritte, entsprechend dem vorgesehenen Zugang, sowohl eine Grundsicherheitsprüfung (Art. 10 Abs. 2 PSPV) als auch eine erweiterte Sicherheitsprüfung (Art. 11 Abs. 2 PSPV) als auch eine erweiterte Sicherheitsprüfung mit Befragung (Art. 12 Abs. 1 PSPV) durchgeführt werden. Es handelt sich somit nicht um eine rechtliche Lücke, sondern vielmehr um eine Frage der Anwendung geltender Vorschriften.

Artikel 14 Absatz 1 Buchstabe c PSPV hält fest, dass für an klassifizierten Projekten ab Stufe VERTRAULICH beteiligte Dritte die Einleitung der PSP vorgenommen wird durch diejenige Stelle, die den Auftrag erteilt, sowie durch Unternehmen mit gültiger Betriebssicherheitserklärung im Rahmen des Geheimschutzverfahrens. Jede Dienststelle, welche Dritten einen klassifizierten Auftrag ab Stufe VERTRAULICH erteilt, ist somit für die Einleitung der stufengerechten PSP zuständig.

Die für die Einleitung der PSP zuständigen Stellen des Bundes nach Artikel 14 Absatz 1 PSPV sind ferner am elektronischen Informationssystem Personensicherheitsprüfung SIBAD nach Artikel 144 ff des Bundesgesetzes über die militärischen Informationssysteme (MIG; SR *510.91*) der Fachstelle PSP VBS angeschlossen (Art. 148 Abs. 1 Bst. c MIG). Die im Rahmen der PSP mit Sicherheitsaufgaben betrauten Ämter des Bundes sind gemäss Art. 148 Abs. 1 Bst. d MIG ebenfalls grösstenteils am System angeschlossen oder können auf Antrag Zugriff erhalten. Im System ist für die angeschlossenen Stellen durch Abrufverfahren ersichtlich, ob und nach welcher Prüfstufe Dritte geprüft wurden und ob die PSP noch gültig ist. Damit können sich die Ämter den notwendigen Überblick verschaffen und bei Notwendigkeit eine neue PSP einleiten.

Der Bundesrat hält fest, dass bezüglich der PSP von Dritten eindeutige Rechtsgrundlagen bestehen und auch die Verantwortlichkeiten grundsätzlich keiner weiteren Klärung bedürfen. Die Departemente und die Bundeskanzlei werden aber ihre zuständigen Stellen ergänzend sensibilisieren.

Empfehlung 6

Die GPDel empfiehlt dem Bundesrat, in seiner Botschaft zum Informationssicherheitsgesetz (ISG) die Rollen, welche die Personensicherheitsprüfung und die Personalführung im Bereich der Informationssicherheit spielen, ausführlich darzulegen und klar voneinander abzugrenzen. Gleichzeitig soll in einem separaten Bericht erläutert werden, wie viele personelle Ressourcen der Bund für die Durchführung der PSP einsetzen soll und welchen Beitrag an den Informationsschutz er damit leisten will.

Der Bundesrat ist damit einverstanden, in seiner Botschaft zum ISG die Rollen, welche die Personensicherheitsprüfung und die Personalführung im Bereich der Informationssicherheit spielen, ausführlich darzulegen und klar voneinander abzugrenzen.

Die personellen Ressourcen, die der Bund für die PSP einsetzt, stehen in direkter Abhängigkeit zu den erforderlichen Sicherheitsprüfungen, welche die Fachstellen im Auftrag des Bundes durchführen. Der heutige Ressourcenbedarf kann sich deshalb vom künftigen Bedarf aufgrund des ISG unterscheiden. Der Bundesrat wird im Rahmen der Botschaft den notwendigen Ressourcenbedarf ausweisen.

Empfehlung 7

Die GPDel empfiehlt dem Vorsteher VBS, dafür zu sorgen, dass der NDB eine neue Unterstellung der Sicherheitszelle ausserhalb der Abteilung NDBU vornimmt. Zugleich ist die Aufgabenverteilung für das Risikomanagement im gesamten Dienst zu überdenken.

Der Bundesrat folgt dieser Empfehlung teilweise. Das VBS überprüft mit dem NDB die organisatorische Frage in einem grösseren Zusammenhang unter Berücksichtigung von Risikomanagement, Qualitätssicherung und der Einhaltung von Vorgaben, Richtlinien und Verhaltensmassregeln (Compliance). Dabei wird auch die Unterstellung der Sicherheitszelle überprüft werden.

Empfehlung 8

Die GPDel empfiehlt dem VBS, dem NDB die Besetzung der Informatikerstellen aus der Personalreserve des Departements bereits im Jahr 2013 zu ermöglichen, obwohl der Bundesrat diese Stellen erst ab 2014 bewilligt hat.

Das VBS hat dem NDB bereits in der ersten Hälfte des Jahres 2013 die Finanzierung von acht Stellen zur Erhöhung der Informatiksicherheit bewilligt, die in der Zwischenzeit mehrheitlich besetzt werden konnten. Allerdings benötigt der Ausbau der Informatiksicherheit bzw. die Rekrutierung von spezialisierten IKT-Fachkräften unter den gegebenen Rahmenbedingungen des Bundes einige Zeit. Nach heutigem Stand wird der NDB bis 1.1.2014 alle acht Stellen besetzen können.

Empfehlung 9

Die GPDel empfiehlt dem Bundesrat, Vorschläge zu erarbeiten, um das Verfahren zur Überprüfung des Standes der Informatiksicherheit im Bund zu verbessern. Die Massnahmen sollen den Bundesrat befähigen, im Rahmen eines institutionalisierten Verfahrens Risiken in der Informatiksicherheit rechtzeitig zu erkennen, die notwendigen risikomindernden Massnahmen zu beschliessen und ihre Umsetzung zu verfolgen.

Der Bundesrat ist bereit, diese Empfehlung entgegen zu nehmen und insbesondere das Verfahren zur Überprüfung des Standes der IKT-Sicherheit in der zentralen Bundesverwaltung weiter zu entwickeln.

In der IKT-Sicherheit in der Bundesverwaltung werden Vorgaben, Umsetzung und Controlling unterschieden.

Gestützt auf die Bundesinformatikverordnung (BinfV; SR *172.010.58*) erarbeitet das Informatiksteuerungsorgan des Bundes (ISB) Vorgaben, die vom Bundesrat bzw. deren Details vom ISB verabschiedet werden. Diese Vorgaben stützen sich auf eine laufend aktualisierte Bedrohungs- und allgemeine Schutzbedarfsanalyse. Die Umsetzung der Vorgaben liegt im Zuständigkeitsbereich der betroffenen Departemente und Verwaltungseinheiten (Linienverantwortung, Art. 9 Abs. 1 und Art. 10 BinfV). Der Linie obliegt auch die interne Kontrolle der Umsetzung, während die Eidgenössische Finanzkontrolle als IKT-Revisionsstelle die Verantwortungswahrnehmung der Linie überprüft (Art. 28 BinfV).

Zur Unterstützung des Bundesrates in der Wahrnehmung seiner Gesamtverantwortung über den Einsatz der IKT in der Bundesverwaltung (Art. 14 BinfV) unterbreitet ihm das ISB anhand der Selbstdeklaration der Departemente das jährliche Reporting (Controlling) und stellt wo nötig Anträge zur Verbesserung (Art 11 BinfV). Aufbauend auf diesem Verfahren, das auch im Bericht der GPDeI zusammen mit den Prüfungen der EFK als zielführend bewertet wird, ist der Bundesrat bereit, die Verfahren weiter zu entwickeln und damit die Empfehlung der GPDeI umzusetzen.

Empfehlung 10

Die GPDel empfiehlt dem Bundesrat, unter der Federführung des Eidg. Personalamtes (EPA), eine interdepartementale Arbeitsgruppe einzusetzen, deren Aufgabe es ist, besondere Anstellungsbedingungen zu erarbeiten, welche es erlauben, in der Personalführung die Reaktionsmöglichkeiten gegenüber Innentäterrisiken zu verbessern. Um bei den betroffenen Mitarbeitenden die dafür notwendige Akzeptanz zu schaffen, wären insbesondere auch finanzielle und andere Kompensationsmassnahmen zu prüfen. Der Bundesrat soll bis Ende 2014 zu den Resultaten der Arbeitsgruppe Stellung nehmen.

Das geltende Personalrecht sieht schon heute die Möglichkeit der Freistellung vom Dienst vor. Diese Massnahme kann sowohl während dem ungekündigten Arbeitsverhältnis (Art. 103 Bundespersonalverordnung, BPV; SR *172.220.111.3*) als auch nach erfolgter Kündigung (Art. 103*a* BPV) vorgenommen werden. In ihrem Bericht möchte die GPDeI insbesondere die Möglichkeit zur raschen Freistellung während

des ungekündigten Arbeitsverhältnisses erweitern. Artikel 103 Absatz 1 BPV sieht die folgenden Bedingungen für eine Freistellung während des ungekündigten Arbeitsverhältnisses vor:

«[1] Ist eine korrekte Aufgabenerfüllung gefährdet, so kann die zuständige Stelle nach Artikel 2 die angestellte Person sofort vorsorglich vom Dienst freistellen oder sie in einer anderen Funktion verwenden, wenn:

a. schwere strafrechtlich oder disziplinarisch relevante Vorkommnisse festgestellt oder vermutet werden;

b. wiederholte Unregelmässigkeiten erwiesen sind; oder

c. ein laufendes Verfahren behindert wird.»

Empfehlung 11

Die GPDel fordert den Vorsteher VBS auf, ausnahmslos für die Respektierung der Einsichtsrechte der ND-Aufsicht, die von Gesetz (Art. 8 ZNDG i.V.m. Art. 26 Abs. 1 BWIS) und Verordnung (Art. 33 Abs. 1 V-NDB) garantiert werden, zu sorgen. Der NDB kann diese Informationsrechte weder alleine noch im Einverständnis mit dem Departementsvorsteher einschränken.

Die Frage der Kompetenzen und Leistungen des VBS-internen Kontrollorgans über die Nachrichtendienste wurde vom VBS bereits im Herbst 2012 aufgenommen. Die Erarbeitung des neuen Nachrichtendienstgesetzes (NDG) und die Datenentwendung im Nachrichtendienst veranlassten den Chef VBS, die Voraussetzungen einer wirksamen Kontrolle über den NDB und die Leistungsfähigkeit der seit Anfang 2009 bestehenden Nachrichtendienstlichen Aufsicht (ND-Aufsicht) von einem externen Sachverständigen überprüfen zu lassen. Prof. Dr. Heinrich Koller, ehemaliger Direktor des Bundesamtes für Justiz, wurde mit dieser Aufgabe betraut. Die Studie hat unter anderem geklärt, wie die Leistungsfähigkeit der ND-Aufsicht in der heutigen Organisationsform zu beurteilen ist und ob die ND-Aufsicht über die erforderlichen Mittel und Rechte verfügt.

Die Rechte und Pflichten sowie insbesondere das umfassende Auskunftsrecht der ND-Aufsicht wurden in den Art. 31–34 der Verordnung des Bundesrates über den Nachrichtendienst des Bundes (V-NDB; SR *121.1*) festgehalten und in den departementsinternen Weisungen des Chefs VBS über die Nachrichtendienstliche Aufsicht vom 20. Januar 2011 präzisiert. Entsprechend sind die Mitarbeiterinnen und Mitarbeiter des NDB gegenüber der ND-Aufsicht zu wahrheitsgetreuer und vollständiger Auskunft verpflichtet. In Ergänzung dessen empfahl Prof. Koller in seinem Abschlussbericht von Ende März 2013, den Stellenwert der ND-Aufsicht departementsintern zu erhöhen, den direkten Zugang zum Chef VBS zu vereinfachen und die Unabhängigkeit in der Aufgabenerfüllung auf formell-gesetzlicher Stufe zu verankern.

In Umsetzung dieser Empfehlungen ordnete der Chef VBS Ende April 2013 einen Katalog mit umfassenden Massnahmen zur Stärkung der ND-Aufsicht an. Als wichtigste Massnahme wird die Unabhängigkeit der ND-Aufsicht in der Auftragserledigung auf formell-gesetzlicher Stufe im neuen ND-Gesetz festgehalten. Art. 66 E-NDG wird wie folgt ergänzt: «Sie [die ND-Aufsicht] ist in der Erfüllung ihrer Kontrollaufgaben weisungsungebunden». Für den Bundesrat ist entscheidend, dass

die ND-Aufsicht, welche die Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit der Nachrichtendienste prüft, ihre Schlüsselfunktion unabhängig und wirksam erfüllen kann. In diesem Sinne nimmt der Bundesrat diese Empfehlung entgegen.

4 Schlussfolgerungen

Eine Berichterstattung über offensichtliche Mängel in einem Teilbereich des Nachrichtendienstes, ohne auch dessen Gesamtleistungen anzuerkennen, steht im Gegensatz zur tatsächlichen Wahrnehmung seiner Auftraggeber und Leistungsbezüger. Der Bundesrat stellt fest, dass auch das Vertrauen ausländischer Partner in den NDB seit der Fusion gewachsen ist.

Ein Nachrichtendienst muss bei seiner Arbeit immer Risiken abschätzen, seien diese politischer, rechtlicher, menschlicher oder technischer Natur. Nach der von den parlamentarischen Aufsichtsorganen angestossenen Fusion des Inland- und Auslanddienstes ist es nach Ansicht des Bundesrates dem neuen Dienst gelungen, ohne Wissensverluste oder gravierende personelle Probleme die Rechtmässigkeit seiner Arbeit sicherzustellen, eine gemeinsame Arbeitskultur zu etablieren und gleichzeitig die Leistung mit hoher Qualität weiterzuführen.

Dass im untersuchten Fall die Reaktion spät – nach Auffassung der GPDel zu spät – erfolgte, ist zum Anlass zu nehmen, die Lehren im NDB und in der Bundesverwaltung zu ziehen. Der dem Bericht zugrunde liegende Fall zeigt exemplarisch die Schwierigkeiten auf, Zielkonflikte zwischen den Pflichten des Arbeitgebers, den Rechten des Arbeitsnehmers sowie staatlichen Sicherheits- und Geheimhaltungsinteressen rechtzeitig zu erkennen und wirksam zu lösen.