Immer noch Mängel beim NDB II

5. Februar 2014

Anfang Februar 2014 wurde der Jahresbericht der Geschäftsprüfungskommissionen und der Geschäftsprüfungsdelegation (GPDel) der eidgenössischen Räte vom 31. Januar 2014 vorgestellt. Im VBS von Ueli Maurer läuft vieles schief. Die Staatsschutzdatenbank, welche angeblich per Ende 2012 bereinigt wurde, enthält immer noch unzulässige Einträge wie Verwaltungsdaten, Medien und gelöschte Meldungen. Zudem werden BWIS-Daten zum Teil immer noch doppelt erfasst. Auszüge des Berichts der GPDel schildern von unbrauchbaren Gesetzestexten über die noch immer nicht bereinigte Staatsschutzdatenbank ISIS01 und die fehlende Trennung von Staatsschutz- und Verwaltungsdaten weiter zu unzulässiger Aufbewahrung von Kopien gelöschter Meldungen und einem unnützen System «Fotopass» bis zur Informatiksicherheit viele Ungereimtheiten. Die grössten Schnitzer sind unten kurz zusammengefasst, der vollständige Text der einzelnen Kapitel ist über die Links abrufbar.

4.1.4 Qualitätssicherung bei nicht veröffentlichten Rechtstexten

Erlasse und völkerrechtliche Verträge können zum Schutz der inneren und äusseren Sicherheit geheim gehalten werden. Allerdings muss die GPDel jedes Jahr über Titel und Inhalt der im Vorjahr nicht publizierten Rechtstexte orientiert werden. Im Verlauf der letzten Jahre musste aber die GPDel nach der Prüfung einzelner nicht publizierter Erlasse feststellen, dass eine verlässliche Qualitätskontrolle nicht gewährleistet ist. In einem Fall war ein Erlass materiell derart ungenügend, dass die GPDel in Zusammenarbeit mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) eine Revision mit dem Ziel einer völligen Neuformulierung verlangen musste. In allen Fällen ging es um Unterlagen oder Erlasse des VBS.

4.2.1 Entwicklung des Datenbestands in ISIS

Als Folge der von der GPDel verlangten Überprüfungen des Staatsschutzinformationssystems ISIS verringerte sich die Zahl der in ISIS registrierten Personen und Drittpersonen um vier Fünftel. Mitte 2013 waren in ISIS noch rund 36,000 Personen und 5,000 Drittpersonen registriert. Dieser Bestand veränderte sich bis Ende 2013 nur unwesentlich.

Die Zahl der Institutionen sank im Jahr 2013 unter die Schwelle von 10,000. Diese Zahl, welche auch Drittinstitutionen enthält, hatte Ende 2010 noch rund 16,000 betragen.

Im Jahr 2009 hatte das BVGer die Registrierung von Medien (z. B. Zeitungen) als eigenständige ISIS-Objekte kritisiert. Im Rahmen ihrer Nachkontrolle zur ISIS-Inspektion stellte die GPDel fest, dass sich im Gegensatz zu den anderen Einträgen in ISIS die Zahl der Medien bis Ende 2011 kaum verändert hatte. Bis Ende 2013 sank die Zahl dann auf rund 60 Einträge. Die GPDel stiess aber auf einzelne Fälle, die nach den Kriterien, die das BVGer im Jahr 2009 aufgestellt hatte, offensichtlich nicht in ISIS registriert sein dürfen. Daraus schliesst die GPDel, dass der NDB die vom BVGer verlangte Überprüfung der in ISIS registrierten Medien noch nicht abschliessend vorgenommen hat.

4.2.2 Trennung von Staatsschutz- und Verwaltungsdaten

In der Empfehlung 6 ihres ISIS-Berichts empfahl die GPDel dem Bundesrat, sicherzustellen, dass nur staatsschutzrelevante Informationen und keine Verwaltungsdaten in der Datenbank Staatsschutz (ISIS01) abgelegt werden. Als Folge der Empfehlung der GPDel erliess der Direktor NDB am 1. Juni 2011 eine Weisung betreffend die Bearbeitung von Daten in ISIS02. Die Weisung schrieb vor, dass Verwaltungsdaten nur mehr in der Datenbank ISIS02 und nicht mehr in ISIS01 abzulegen waren. Die Weisung hatte jedoch keine Wirkung auf die Verwaltungsdaten, die bereits früher fälschlicherweise in ISIS01 Eingang gefunden hatten. Der NDB hat Ende 2012 ein Geschäftsverwaltungssystem (GEVER NDB) eingeführt, um ISIS02 zu ersetzen. Eingehende administrative Unterlagen werden seither im neuen GEVER NDB und nicht mehr in ISIS02 abgelegt. Die bereits in ISIS02 abgelegten Verwaltungsdaten sollen im Rahmen der Ablösung des gesamten Systems ISIS ins neue GEVER NDB migriert werden. Verwaltungsdaten in ISIS01 werden erst mit der Stilllegung von ISIS ins GEVER NDB verschoben werden.

4.2.3 Unzulässige Aufbewahrung von Kopien gelöschter Meldungen in der ISIS-Verwaltungsdatenbank

Die Weisung des Direktors NDB vom 1. Juni 2011 betreffend ISIS02 sah vor, dass «Berichte, die einen in der Datenbank Staatsschutz [ISIS01] dokumentierten Verdacht entkräften, zusammen mit dem verdachtsbegründenden Bericht in der [Datenbank] Verwaltung erfasst [werden]». Dies bedeutete in letzter Konsequenz, dass die Meldung, welche den Anlass für die Registrierung einer Person in ISIS gegeben hatte, zwar in ISIS01 gelöscht, zuvor aber noch als Kopie in ISIS02 abgelegt wird. Die Meldungen würden somit trotz ihrer Entfernung aus ISIS01 der vollständigen Löschung entgehen.

Im April 2013 besprach die GPDel diese Problematik mit der ND-Aufsicht. Diese erklärte der GPDel, dass sie mit dem Einverständnis des Vorstehers VBS einen «runden Tisch» mit dem BJ und dem EDÖB einberufen werde, um mit dem NDB die Rechtsgrundlagen für die Datenbearbeitung in ISIS und die Rechtmässigkeit der NDB-internen Regelwerke zu besprechen.

Der «runde Tisch» fand am 10. Juni 2013 statt. Zu seinen Ergebnissen erstellte die ND-Aufsicht am 30. August 2013 einen Bericht zuhanden des Vorstehers VBS, welcher eine neue Weisung des Direktors des NDB betreffend ISIS02 veranlasste.

Laut der neuen Weisung werden Berichte, die einen in der Datenbank ISIS01 dokumentierten Verdacht entkräften, nicht mehr in GEVER NDB gespeichert, sondern in ISIS temporär erfasst und anschliessend zusammen mit den verdachtsbegründenden Informationen gelöscht. In GEVER NDB kann stattdessen eine Aktennotiz abgelegt werden, welche darauf hinweist, dass der NDB in einem bestimmten Zeitraum Daten über die betreffende Person oder Organisation bearbeitet hat.

4.2.4 Pendenzen für das Nachfolgesystem von ISIS

Drei Empfehlungen des ISIS-Berichts der GPDel betreffen das Nachfolgesystem von ISIS. So verlangt die Empfehlung 16, dass ein Nachfolgesystem nur dann in Betrieb genommen wird, wenn mit ihm die gesetzlichen Anforderungen uneingeschränkt erfüllt werden können. Es dürfen zudem nur Daten ins neue System migriert werden, welche allen gesetzlichen Vorgaben entsprechen.

Nach Aussagen der ND-Aufsicht hat der NDB entsprechend der Empfehlung 16 die rechtlichen Anforderungen, die sich für das Nachfolgesystem von ISIS ergeben, in einem Dokument zusammengetragen. Diese Zusammenstellung soll den Stand des geltenden Rechts, d. h. des BWIS in seiner aktuellen Form, reflektieren und floss laut ND-Aufsicht in die Detailspezifikationen des Projektes Informatisiertes Analyse- und Auswertungstool (IASA NDB) ein. Das Nachfolgesystem von ISIS wird im Rahmen dieses Projektes realisiert.

Die zweite Forderung von Empfehlung 16 verlangt, dass die ISIS Daten allen rechtlichen Vorgaben entsprechen müssen, bevor sie ins Nachfolgesystem von ISIS migriert werden. Nach eigenen Angaben hat der NDB die verbleibenden Verwaltungsdaten in der Staatsschutzdatenbank ISIS01 identifiziert und kann gewährleisten, dass sie nicht ins Nachfolgesystem für ISIS, sondern ins Geschäftsverwaltungssystem GEVER NDB migriert werden.

4.2.5 Neuauflage des präventiven Fahndungsprogramms «Fotopass»

Das präventive Fahndungsprogramm Fotopasskontrolle («Fotopass») war in der Zeit des Kalten Krieges als Mittel der Spionageabwehr eingeführt worden und diente u. a. der Überwachung von Schweizer Bürgern, die nach Osteuropa reisten. Nach der Fichenaffäre wurde es auf Angehörige ausgewählter ausländischer Staaten beschränkt, die beim Übertritt an der Schweizer Grenze erfasst wurden.

Die GPDel empfahl dem Bundesrat, das präventive Fahndungsprogramm «Fotopass» einzustellen. In seiner Stellungnahme vom 20. Oktober 2010 stimmte der Bundesrat der Einstellung von «Fotopass» in der bisherigen Form zu und stellte in Aussicht, dass der NDB das bestehende Instrumentarium (Gerätschaften an der Grenze) in einem Nachfolgeprojekt einsetzen werde. Anfang 2013 nahm die GPDel eine Standortbestimmung zum «Fotopass»-Programm vor. Als Schlussfolgerung schrieb sie dem Vorsteher VBS, «dass das Programm weder zweckmässig noch wirksam [sei], demgegenüber jedoch namhafte personelle Ressourcen im NDB [binde], welche in anderen Bereichen des NDB dringend nötig wären». Die GPDel empfahl dem VBS deshalb, den Verzicht auf «Fotopass» ernsthaft in Erwägung zu ziehen.

Als Reaktion auf die erneute Empfehlung der GPDel, das Programm einzustellen, beschloss das VBS abzuklären, wie ein Ausbau des Programms mit neuen technischen Erfassungsmöglichkeiten dessen Zweckmässigkeit verbessern könnte. Eine entsprechende Machbarkeitsstudie sollte unter der Federführung des GWK durchgeführt werden.

4.2.6 Verordnungsrevision macht Umsetzung der Empfehlung 8 rückgängig

Am 29. November 2013 verabschiedete der Bundesrat die vierte Revision der ISVNDB. Seit der Schaffung des NDB bestimmt diese Verordnung die Regeln für die Datenbearbeitung in den verschiedenen Informationssystemen des NDB, insbesondere auch in ISIS.

Revidiert wurde auch Artikel 29 Absatz 2 der Verordnung, der nun bestimmt, dass die für die Datenerfassung zuständigen Mitarbeitenden «beurteilen, ob eine Information Rückschlüsse auf die Staatsschutzrelevanz der von der Information betroffenen Person oder Organisation zulässt. Ist dies der Fall, geben sie die Daten in ISIS ein».

Damit hob der Bundesrat die Änderung von Artikel 29 Absatz 2 ISV-NDB wieder auf, die er am 9. Dezember 2011 vorgenommen hatte, um die Empfehlung 8 der GPDel umzusetzen.

Die GPDel hat wenig Verständnis für derartige Pannen bei der Rechtsetzung und erwartet, dass dieses legislative Versehen rasch behoben wird.

4.2.7 Information des Bundesrats zur Nachkontrolle

Am 18. Dezember 2013 informierte die GPDel den Bundesrat in einem Schreiben über den Stand ihrer Nachkontrolle zur Inspektion ISIS.

Die GPDel wies den Bundesrat auf die letzten offenen Punkte im Zusammenhang mit den Daten hin, die noch aus der ISIS-Staatsschutzdatenbank entfernt werden müssen. Sie brachte dem Bundesrat auch ihre Einschätzung zur Kenntniss, dass die Neuauflage des Fahndungsprogramms «Fotopass», welche der Bundesrat im Nachgang zur ISIS-Inspektion beschlossen hatte, in Bezug auf ihre Zweckmässigkeit nicht befriedigen könne. Weiter machte die Delegation den Bundesrat darauf aufmerksam, dass die Empfehlung 8, die er mit einer Änderung der ISV-NDB im Jahr 2011 umgesetzt hatte, wegen der kürzlich erfolgten Revision der gleichen Verordnung nicht mehr als erfüllt erachtet werden könne.

Wie die GPDel dem Bundesrat schrieb, würde sie ihre Nachkontrolle erst dann abschliessen, wenn auch die noch offenen Empfehlungen umgesetzt worden seien.

4.3 Einhaltung des ZNDG beim Pilotversuch ISAS

Seit der Bundesrat Ende 2009 das Ausführungsrecht zum ZNDG erliess, hat sich die GPDel kritisch mit den dort enthalten Bestimmungen zur Datenbearbeitung auseinandergesetzt.

Da Artikel 19 V-NDB die Ablage der Informationen, die der NDB einerseits über das Ausland und anderseits aufgrund des BWIS beschafft hat, nicht abschliessend regelte, musste der NDB das Verfahren im Verlauf des Jahres 2010 in einer internen Kriterienliste konkretisieren (Art. 19 Abs. 4 V-NDB). Darin sah der NDB vor, dass eine Information sowohl in ISIS als auch in ISAS abgelegt werden konnte.

Wie die GPDel gestützt auf ein Gutachten des BJ feststellte, verletzt diese Praxis jedoch Artikel 6 ZNDG, wenn eine Information, die gestützt auf das BWIS beschafft wurde, nicht nur in ISIS, sondern auch in ISAS abgelegt wird. An einem «runden Tisch» vom 10. Juni 2013 wurde vereinbart, dass der NDB prüfen soll, ob die Doppelerfassungen in ISIS und ISAS für die Aufgabenerledigung des Dienstes zwingend notwendig seien. Zudem beschloss das VBS, dass im Rahmen der laufenden Teilrevision des ZNDG neue Bestimmungen eingeführt werden sollten, um Doppelerfassungen auf formellgesetzlicher Stufe zu regeln.

Die Botschaft zur ZNDG-Revision wurde vom Bundesrat am 14. August 2013 verabschiedet. Der Bundesrat schlug eine neue Bestimmung vor, die unter bestimmten Bedingungen die von der GPDel kritisierten Doppelerfassungen erlaubt. Nach dem Vorschlag des Bundesrats waren aber Daten, die in ISIS und ISAS erfasst wurden, nach den Vorgaben der ISIS-Qualitätskontrolle zu überprüfen.

Rückblickend lässt sich feststellen, dass es mehr als drei Jahre dauerte, bis die verantwortlichen Stellen im VBS konkrete Schritte unternahmen, um die Kritik der GPDel an der Rechtmässigkeit der Doppelablagen in ISIS und ISAS mit konstruktiven Vorschlägen zu beantworten. Völlig gesetzeskonform wird die Praxis der Doppelablagen allerdings erst dann sein, wenn die Teilrevision des ZNDG in Kraft getreten ist.

4.4 Regelung der Archivierung von Unterlagen des NDB im ZNDG

Nachdem der Bundesrat am 14. August 2013 eine Revision des ZNDG beschlossen hatte, lud die Sicherheitspolitische Kommission des Ständerats (SiK-S) als zuständige Legislativkommission die GPDel am 23. August 2013 zu einem Mitbericht ein.

Mit der ZNDG-Revision wollte der Bundesrat in erster Linie die gesetzlichen Grundlagen für das Informationssystem ISAS schaffen. Die GPDel hatte den Pilotversuch mit ISAS, den der NDB Mitte 2010 begonnen hatte, in den letzten Jahren kritisch verfolgt.

Als problematisch erachtete die GPDel die neue Bestimmung, mit welcher der Bundesrat auf Gesetzesstufe Unterlagen, die von ausländischen Partnerdiensten stammen, von der Archivierung im BAR ausnehmen wollte.

Als der Ständerat am 3. Dezember 2013 die Revision des ZNDG beriet, stellte Ständerat Paul Niederberger für die GPDel den Antrag, Absatz 2 von Artikel 7*a* nach dem ursrpünglichen Vorschlag der GPDel zu formulieren. Der Ständerat folgte diesem Antrag.

4.5 Inspektion zur Informatiksicherheit im NDB

Aufgrund ihrer Inspektion stellte die GPDel fest, dass der NDB als Organisation nicht genügend darauf ausgerichtet war, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit zu gewährleisten.

Als der NDB Anfang 2010 seine Arbeit aufnahm, waren die Personalressourcen für die Informatik des neuen Dienstes äusserst knapp bemessen. Dies führte dazu, dass beim Ausfall des einzigen internen Datenbankadministrators die Betriebssicherheit der Datenbanken nur gewährleistet werden konnte, solange keine gravierenden Probleme auftauchten. Diese Personalsituation erschwerte es auch, die Integrität der Datenbankprogramme zu überprüfen.

Die GPDel stellte auch fest, dass der NDB verschiedene Vorschriften für die Informatiksicherheit auf Stufe Bund und VBS nicht eingehalten hatte. Für die Wahrnehmung der Aufgabe des Informatiksicherheitsbeauftragen (ISBO) stand, wenn überhaupt nur in ungenügendem Ausmass Personal zur Verfügung. Die vorgeschriebenen Sicherheitskonzepte für die Anwendungen und Systeme waren mehrheitlich ungenügend oder fehlten. Um den Betrieb aufrechterhalten zu können, wurde in der Informatik des NDB auch darauf verzichtet, die Zugriffsmöglichkeiten auf den Systemen einzuschränken.

Diese Ausgangssituation trug dazu bei, dass der NDB vorgängig zum Datendiebstahl im Mai 2012 nicht angemessen auf verschiedene Anzeichen einer Gefährdung der Verfügbarkeit und Integrität seiner Daten reagieren konnte. Als Folge von Problemen mit dem einzigen internen Datenbankadministrator stand die Leitung der Abteilung vor dem Dilemma, entweder mit seiner Freistellung die Verfügbarkeit der Systeme zu gefährden oder bei seinem weiteren Einsatz ein Risiko für die Integrität und - wie es sich nachträglich auch zeigte - die Vertraulichkeit der Daten in Kauf zu nehmen. Letztlich erlaubte indes die ungenügende Reaktion der zuständigen Abteilung in Sachen Personalführung und Risikomanagement den Datendiebstahl. Der Direktor des Dienstes erfuhr von diesen Problemen erst, nachdem der Datendiebstahl aufgrund eines externen Hinweises intern bestätigt wurde.

Nach dem Datendiebstahl reagierte der NDB mit einer ganzen Reihe von technischen und organisatorischen Massnahmen, um erkannte Mängel in der Informatiksicherheit rasch zu beheben. Diese punktuellen Massnahmen erfolgten indes nicht im Rahmen eines umfassenden Risikomanagements. Das volle Ausmass der Ressourcenproblematik in der Informatik wurde von der Leitung des NDB erst ein halbes Jahr nach dem Vorfall erkannt. Über die notwendigen

Personalkredite entschied der Bundesrat auf Antrag des VBS erst im Frühling 2013, also etwa ein Jahr nach dem Datendiebstahl.

Als Folge des Datendiebstahls im NDB veranlasste der Vorsteher VBS im Herbst 2012 auch eine ad hoc Untersuchung zur Informationssicherheit auf Stufe Bund. Diese Abklärungen überschnitten sich mit dem vom Bundesrat seit Jahren institutionalisierten Reporting zur Informations- und Informatiksicherheit. Den Weg zur Verbesserung der Informatiksicherheit auf Stufe Bund erkennt die GPDel weniger in solchen isolierten Reaktionen auf einen Vorfall, als viel mehr in einer Intensivierung der systematischen Massnahmen, welche der Bundesrat seit 2009 umsetzen und kontrollieren lässt.

Im April 2013 publizierte das VBS in eigener Verantwortung seine abschliessende Würdigung zum Datendiebstahl im NDB. Die Inspektion der GPDel hat zum Teil andere Erkenntnisse ergeben. Die GPDel konnte auch die Schlussfolgerungen des VBS zur Informationssicherheit auf Stufe Bund nicht alle teilen.