Mai 2014

stiftung | neue verantwortung

POLICY BRIEF

Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle

Dr. Stefan Heumann & Dr. Thorsten Wetzling

PRIVACY PROJECT

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle

Dr. Stefan Heumann
stellv. Programmleiter
„Europäische Digitale Agenda“

Dr. Thorsten Wetzling
Senior Research Fellow
Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)

Einleitung[1]

Es ist jetzt beinahe ein Jahr her, seit die Enthüllungen von Edward Snowden den mächtigsten Geheimdienst der Welt in den Mittelpunkt des öffentlichen Interesses gerückt haben. Vor allem in Deutschland war und ist die Empörung groß. Zu Recht will man hierzulande nicht hinnehmen, dass die Massenüberwachungsprogramme der NSA unsere Privatsphäre und unsere Grundrechte massiv verletzen. Die Beschwichtigungen der amerikanischen Regierung, dass ihre Geheimdienste strengen Gesetzen und Kontrollen unterliegen, haben die Kritiker bisher nicht überzeugen können. Selbst wenn man davon absieht, dass die Gesetze vage und die Kontrolle der Dienste unzureichend ist, bleibt doch festzuhalten, dass der amerikanische Rechtsstaat und seine Institutionen vor allem darauf ausgelegt sind, die Rechte von sogenannten US-Personen, also amerikanischen Staatsbürgern oder Personen, die sich in den Vereinigten Staaten aufhalten, zu schützen. Die Massenüberwachungsprogramme, die zum Beispiel deutsche oder europäische Bürger betreffen, unterliegen weit weniger strengen Regeln. Hier hat der amerikanische Geheimdienst National Security Agency (NSA) weitgehend freie Hand.

Bei aller berechtigten Kritik an den amerikanischen Massenüberwachungsprogrammen ist in Deutschland bisher zu selten die Frage gestellt worden, wie eigentlich der Bundesnachrichtendienst (BND) im Gegenzug mit der Überwachung von Nicht-Deutschen umgeht. Diese Frage ist alles andere als trivial. Schließlich ist unsere Kritik an den Amerikanern nur wenig glaubwürdig, wenn auch unsere eigenen Gesetze und Kontrollinstanzen bei der nachrichtendienstlichen Überwachung von Kommunikationsverkehren Ausländern weniger Rechte als Inländern zubilligen.

Dank Edward Snowden sind wir allerdings in der paradoxen Lage, dass wir mehr über die amerikanischen Geheimdienst als unsere eigenen nachrichtendienstlichen Praktiken wissen. Eine Auseinandersetzung mit unseren eigenen Praktiken ist aber notwendig, um mit den Vereinigten Staaten und europäischen Partnern eine Debatte über rechtsstaatliche Standards für nachrichtendienstliche Tätigkeiten im digitalen Zeitalter führen zu können. Denn Eines haben die Enthüllungen von Edward Snowden uns allen deutlich vor Augen geführt: wir brauchen diese Debatte dringend, da Digitalisierung und technologischer Fortschritt Geheimdiensten Möglichkeiten zur Spionage und Überwachung geschaffen haben, die vor wenigen Jahren noch undenkbar schienen.

Wir wollen mit diesem Arbeitspapier einen Beitrag dazu leisten, diese Debatte in Deutschland in Gang zu bringen. Uns interessiert daher vor allem, wie der BND mit Fragen umgeht, die bei der NSA im Mittelpunkt der Kritik stehen. Wir haben daher den Untersuchungsgegenstand des Papiers auf das, was im Fachjargon die Überwachung des „offenen Himmels“ oder die strategische Auslandsaufklärung genannt wird, konzentriert. Hierbei handelt es sich um die massenhafte Überwachung von Kommunikationsverkehren von Ausländern im Ausland. In der Regel werden diese Kommunikationsverkehre in automatisierten Prozessen mit Suchbegriffen gefiltert, um gegebenenfalls nachrichtendienstlich relevante Daten und Inhalte identifizieren zu können.

Wir gehen in unserer Untersuchung zur strategischen Auslandsaufklärung in vier Schritten vor. Im ersten Kapitel beschreiben wir kurz die technischen Möglichkeiten, die aufgrund der gemeinhin unter dem Schlagwort Digitalisierung zusammengefassten informationstechnologischen Revolution heutzutage zur Verfügung stehen. Im zweiten Kapitel werden die historischen Ursprünge der sogenannten „Überwachungsgesetze“ untersucht. Im dritten Kapitel stehen die

1 Die Autoren bedanken sich bei Prof. Niko Härting, Dr. Bertold Huber, Jan-Peter Kleinhans und Dr. Dominic Hörauf für die kritischen Kommentare und wertvollen Anregungen zu einer früheren Fassung dieses Textes. Ihr Dank gilt ferner den Teilnehmern der Werkstattgespräche „Rechtlichen Grenzen nachrichtdienstlicher Überwachung“ am Walter-Hallstein-Institut für Europäisches Verfassungsrecht in Berlin für die wichtigen Gedankenanstöße. Für den Inhalt dieser Studie sind die Autoren allein verantwortlich.

rechtlichen Grundlagen für die Befugnisse und Kontrolle der strategische Auslandsaufklärung des BND im Mittelpunkt. Dabei konzentrieren wir uns insbesondere auf das G-10 Gesetz. Schließlich diskutieren wir im vierten Kapitel die wichtigsten Aspekte der parlamentarischen Kontrolle.

Wir beanspruchen mit diesem Papier nicht, eine umfassende und abschließende Untersuchung vorgelegt zu haben. Dies ist gar nicht unser Anliegen. Es geht uns primär darum, die hier diskutierten Fragen und Probleme einem breiteren Publikum zugänglich zu machen. Fragen nach den rechtlichen Grundlagen und der parlamentarischen Kontrolle der Nachrichtendienste bedürfen dringend einer breiteren öffentlichen Debatte. Schließlich geht es hier um den Schutz unserer Grundrechte und die Funktionsfähigkeit unseres Rechtsstaats. Drei in diesem Papier identifizierte Problembereiche unterstreichen die Dringlichkeit und die Relevanz der hier aufgeworfenen Fragen. Erstens hat auch in Deutschland der rechtliche Rahmen nicht mit den technologischen Entwicklungen Schritt gehalten. Die rechtliche Eingrenzung der Befugnisse zur strategischen Auslandsüberwachung ist daher völlig unzureichend. Zweitens praktizieren auch die deutschen Dienste, was wir den Amerikanern vorwerfen: Die gesetzlichen Vorgaben sind fast ausschließlich auf den Grundrechtsschutz der eigenen Bürger ausgerichtet, während es für die Überwachung von Ausländern viel geringere rechtliche Hürden gibt. Drittens ist die parlamentarische Kontrolle der Nachrichtendienste in Deutschland völlig unzureichend. Diese und weitere hier diskutierte Probleme bedürfen dringend einer breiteren gesellschaftlichen und politischen Debatte. Letztlich liegt es vor allem in der Verantwortung des Bundestags, diese Probleme aufzugreifen.

1. Digitalisierung und technische Aufklärung

Das Ausmaß der von Edward Snowden enthüllten Überwachungsprogramme hat viele überrascht. Mehrere Faktoren haben maßgeblich zur Ausweitung geheimdienstlicher Überwachung im letzten Jahrzehnt geführt. Die terroristischen Anschläge vom 11. September haben amerikanische Geheimdienste massiv unter Druck gesetzt. Ihnen wurde vorgeworfen, versagt zu haben. Zugleich rückte der internationale Terrorismus immer mehr in den Fokus. Während vor wenigen Jahrzehnten Geheimdienste sich hauptsächlich für staatliche Akteure und strategisch wichtige Wirtschaftszweige interessierten, gehört die Aufdeckung von terroristischen Netzwerken heutzutage zu den Kernaufgaben. Hierfür halten viele Sicherheitsexperten es für notwendig und legitim, breite Bevölkerungsschichten zu überwachen, um möglicherweise verdächtige Verhaltensmuster zu identifizieren. Massenüberwachung im großen Stil wurde aber erst durch die technologischen Entwicklungen möglich, die hier kurz skizziert werden sollen. Ein entscheidender Faktor dabei ist, dass mit dem rasanten Anstieg der Internetnutzung und der Verbreitung von Smartphones die Kosten für Überwachung drastisch gesunken sind. Früher hätten Nachrichtendienste einen enormen Aufwand betreiben müssen, um Kommunikationsverhalten, Interessen und Aktivitäten zu recherchieren, auf die sie heute mit vergleichsweise geringem Einsatz im großem Stil zugreifen können.[2]

Bei Geheimdiensten kann man grundsätzlich zwischen zwei Methoden zur Informationsbeschaffung unterscheiden: menschliche Quellen und technische Aufklärung. Im Rahmen dieses Papiers behandeln wir ausschließlich Fragen in Bezug auf die technische Aufklärung. Hierbei beschränken wir uns wiederum auf strategische Überwachung, die von Individualmaßnahmen zu unterscheiden ist. Während bei Individualmaßnahmen gezielt Kommunikationsverkehre von bestimmten Personen oder Gruppen angezapft werden, bezieht sich die strate-

2 Viele Daten waren im „vor-digitalen“ Zeitalter entweder gar nicht verfügbar oder mussten mit riesigem Aufwand recherchiert und beschafft werden, während heutzutage z. B. nur der Zugriff auf ein Smartphone soziale Netzwerke, intime persönliche Kommunikation oder Aufenthaltsorte offenbaren kann.

gische Überwachung auf das allgemeine Überwachen von Kommunikationsströmen, aus denen geheimdienstlich relevante Kommunikationsverkehre herausgefiltert werden. Vier Faktoren spielen in Bezug auf die Fähigkeiten zur technischen Aufklärung eine besondere Rolle:

1. Verfügbarkeit von technisch basierten Kommunikationsverkehren: die technische Aufklärung kann in großem Umfang nur zum Einsatz kommen, wenn Kommunikationsverkehre und Daten technisch übertragen werden und Geheimdiensten sich daher die Möglichkeit zum Mitschneiden bietet.

2. Zugang zu Kommunikationsverkehren und Daten: dieser Faktor ist in der Regel geographisch determiniert, insbesondere wenn das Abschöpfen von Daten direkten Zugang zu Übertragungsleitungen oder Datenspeichern verlangt. Selbst Funk- und Sattelitenverbindungen sind in ihrer geographischen Reichweite begrenzt und schränken damit Überwachungsmöglichkeiten geographisch ein.

3. Technische Möglichkeiten der Datenauswertung: bei der technischen Aufklärung fallen große Datenmengen an. Hier stoßen Auswertung und Analyse allein durch menschliche Arbeit schnell an ihre Grenzen. Je größer die Datenmengen umso wichtiger werden technische Lösungen zur vollautomatischen Verarbeitung und Auswertung der Daten.

4. Speicherkapazitäten: bei der technischen Aufklärung können riesige Datenmengen anfallen. Die Auswertung dieser Datenmengen setzt voraus, dass man die Daten zumindest temporär speichern kann. Viele Analysemethoden entwickeln allerdings erst dann ihre volle Effektivität, wenn auch langfristig auf die Daten zugegriffen werden kann, um sie mit anderen Datensätzen verknüpfen zu können.

1.1 Verfügbarkeit und Zugang

Anhand der vier Faktoren lassen sich gut die revolutionären technologischen Veränderungen der letzten Jahrzehnte und ihre Auswirkungen auf die Möglichkeiten technischer Aufklärung im digitalen Zeitalter aufzeigen. Während des Kalten Krieges war die Verfügbarkeit von Kommunikationsverkehren für geheimdienstliche Massenüberwachung hauptsächlich auf Festnetztelefonate, Telegramme und satelliten-basierte Kommunikation beschränkt. Wenn zum Beispiel kein Telefonnetz vorhanden ist, begrenzt dies massiv die Möglichkeiten, Gesprächsverkehre in großem Umfang zu überwachen. Telefonüberwachung hingegen erfordert zum Mithören von Gesprächen nur einen Zugriff auf die Übertragungsleitungen. Da beim Telefon das Gespräch bereits technisch aufgefangen wird, muss in den jeweiligen Haushalten nicht eigens eine Aufzeichnungstechnik installiert werden. Dies heißt aber zugleich, dass Gespräche innerhalb des Hauses, die nicht über Telefon geführt werden, mit dieser Technik nicht zu erfassen sind. Deshalb gilt: umso mehr Kommunikation über technische Hilfsmittel stattfindet, desto mehr Möglichkeiten bieten sich für Überwachung durch strategische, technische Aufklärung.

Heutzutage findet durch den Einsatz von moderner Informations- und Telekommunikationstechnologie nicht nur viel mehr Kommunikation vermittelt über technische Geräte statt, sondern durch neue Kommunikationsformen wie soziale Medien werden auch ganz neue Daten- und Kommunikationsströme generiert, die das Interesse von Geheimdiensten wecken können. Mobilfunk hat sich in den letzten Jahrzehnten rasant um den Erdball verbreitet. Über die Kommunikationsinhalte hinaus verraten Verbindungsdaten nicht nur das Netzwerk

an Kontakten, sondern auch den Standort.[3] 1995 steckte das Internet mit weltweit 16 Millionen Nutzern noch in den Kinderschuhen.[4] Im Jahr 2014 wird die Zahl der Internetnutzer auf über 3 Milliarden ansteigen. Die Nutzung von Internetdiensten ist mit einer Aufzeichnung und Übertragung einer Vielzahl von neuen Daten und Informationen über Interessen, Verhalten und soziale Netzwerke verbunden. Kommunikation findet per Email, über soziale Netzwerken und mit speziellen Chat Programmen statt. Geschäfte werden in immer größeren Umfängen über Online-Plattformen abgewickelt. Nachrichten, Information und Unterhaltung erreichen Menschen zunehmend über das Internet. Die Verfügbarkeit von technisch basierten Kommunikationsverkehren und persönlichen Daten ist mit zunehmender Digitalisierung aller Lebensreiche in den letzten Jahrzehnten geradezu explodiert. Hier haben sich für Geheimdienste innerhalb weniger Jahre neue Möglichkeiten der Überwachung eröffnet, die vor wenigen Jahren noch undenkbar schienen.

Während die Verfügbarkeit von Kommunikationsverkehren und Daten in den letzten Jahrzehnten exponentiell zugenommen hat, veränderte sich auch der Zugang zu diesen Daten. Die wichtigste Entwicklung ist dabei die Konvergenz hin zu internetbasierten Übertragungstechnologien. Die Email hat die Bedeutung von Brief und Fax stark zurückgedrängt. Auch die Satellitenübertragung hat massiv an Bedeutung verloren. Selbst Telefonate werden mittlerweile zunehmend über das Internet übertragen.[5] Das Internet ist in den letzten beiden Jahrzehnten zur zentralen globalen Infrastruktur für Kommunikations- und Datenübertragung geworden. Geographie bleibt dabei von entscheidender Bedeutung. Wer direkten Zugang zu den großen Internetknoten oder den großen Unterseekabeln hat, die verschiedene Kontinente und Regionen mit einander vernetzen, hat damit direkten Zugriff auf unvorstellbare Mengen an Kommunikations- und Datenverkehren.[6] Hinzu kommt, dass die Internetknoten auch direkten Zugang zu Datenverkehren aus dem Ausland liefern. Aufgrund der Struktur des Internets und der Globalisierung der internetbasierten Dienste werden in der Regel auch Kommunikations- und Datenverkehre zwischen zwei Standorten in einem Land über internationale Netzverbindungen geroutet. Wer einen der großen Netzknoten im eigenen Land hat, kann daher auf große internationale Kommunikations- und Datenverkehre zugreifen, ohne außerhalb der eigenen Landesgrenzen technische Operationen durchführen zu müssen.[7]

1.2 Rechen- und Speicherkapazitäten

Die ersten beiden Faktoren schaffen die Voraussetzung dafür, dass Geheimdienste mithilfe von technischer Aufklärung Zugriff auf riesige Mengen an Kommunikations- und Datenverkehren erlangen können. Zum einen werden einhergehend mit der Digitalisierung immer mehr Daten generiert. Zum anderen werden diese hauptsächlich über das Internet übertragen. Das Internet ist hierbei als eine globale Infrastruktur von einer Vielzahl von zusammengeschlossenen autonomen Netzwerken zu verstehen, deren zentrale Verbindungsknoten vor allem in Nordamerika und Westeuropa konzentriert sind. Große Datenmengen sind allerdings von geringem Nutzen, wenn man diese nicht verarbeiten und analysieren kann. Gordon Moore stellte 1965 die These auf, dass sich die Leistungsfähigkeit von Mikroprozessoren innerhalb von ein bis zwei Jahren ständig verdoppelt.[8] Diese Voraussage hat sich in den letzten Jahren mit erstaunlicher Konstanz bestätigt und zu einer Multiplikation der Rechenkapazitäten geführt. Damit sind in den letzten Jahren die technologischen Voraussetzungen geschaffen worden, über

3 http://www.globalresearch.ca/why-spying-on-metadata-is-even-more-intrusive-than-listening-to-content/5365133 und http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html
4 http://www.internetworldstats.com/emarketing.htm
5 http://www.teltarif.de/telekom-all-ip-ngn-kunden-migration/news/36256.html
6 http://www.submarinecablemap.com/
7 Eine Auflistung der größten Internetknoten ist auf folgender Seiten einsehbar: http://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size
8 http://de.wikipedia.org/wiki/Mooresches_Gesetz

vollautomatische Computerprogramme riesige Datenmengen innerhalb kürzester Zeit verarbeiten und analysieren zu können. Die technische Verarbeitung und Analyse riesiger Datenmengen verlangt nicht nur hohe Rechenkapazitäten, sondern auch entsprechende Speicherkapazitäten. In der Vergangenheit mussten Daten zu Auswertungszwecken zumindest zwischengespeichert werden. Es sind aber mittlerweile auch Technologien auf dem Markt, die Echtzeit-Analysen großer Datenmengen ermöglichen.[9] Aber selbst beim Einsatz von Echtzeit-Analysen zum Überwachung großer Datenströme werden Speicherkapazitäten spätestens dann notwendig, wenn es darum geht, Daten für die weitere Auswertung zumindest temporär zu speichern.[10] So wurde zum Beispiel im Rahmen der Enthüllungen von Edward Snowden bekannt, dass amerikanische und britische Geheimdienste mit ihren breit angelegten Überwachungsprogrammen vor allem in Bezug auf die Datenspeicherung an ihre technischen Grenzen gestoßen sind. Im Rahmen des Tempora Programms, das der britische Nachrichtendienst GCHQ zur Überwachung der großen Überseeglasfaserleitungen einsetzt, wird der gesamte Datenverkehr jeweils für drei Tage gespeichert und Verbindungsdaten für bis zu 30 Tage. Daten, die von Analysten oder entsprechenden Programmen der Geheimdienste speziell ausgewählt werden, werden sogar noch länger gespeichert. Die NSA hat jüngst für geschätzte 2 Milliarden US Dollar ein neues Daten- und Rechenzentrum in Utah errichtet, um die riesigen Datenmengen aus ihren Überwachungsprogrammen verarbeiten und speichern zu können.

1.3 Upstream, Downstream und spezielle Operationen

Vor allem der amerikanische Geheimdienst NSA und der britische Geheimdienst GCHQ haben sich in den letzten Jahren die oben beschriebenen technologischen Entwicklungen zunutze gemacht, um ihre Fähigkeiten in der technischen Aufklärung massiv auszubauen. Dabei können grundsätzlich zwischen drei Methoden der technischen Aufklärung unterschieden werden: Upstream, Downstream und spezielle Operationen. Unter Upstream wird das Überwachen der großen Datenströme im Internet verstanden. Operativ heißt dies, dass sich Geheimdienste Zugang zu den Internetknoten oder Überseeleitungen verschaffen, um dort die Datenströme mitzuschneiden und für relevant erachtete Kommunikationsverkehre und Verbindungsdaten herauszufiltern und gegebenenfalls zu speichern. Als Downstream bezeichnet man den Zugriff auf Daten, die bei Telekommunikationsanbietern und Internetfirmen gespeichert sind. Laut den von Edward Snowden enthüllten Dokumenten geschieht dies auf zweierlei Weise. Zum einen können die Geheimdienste vor Geheimgerichten nationale Sicherheitsbriefe beantragen und mit diesen von Unternehmen zur Herausgabe von Daten verlangen. Zum anderen hat sich die NSA auch Zugang zu den Leitungen, die Datenzentren von großen Internet Firmen wie Yahoo und Google verbinden, verschafft, um, ohne deren Wissen oder Einverständnis, direkt auf dort gespeicherte Nutzerdaten zugreifen zu können. Schließlich sind NSA und GCHQ auch in der Lage, sich mit Spezialoperationen im Internet weltweit Zugang zu digitalen Informationen zu verschaffen. Hierbei werden unter anderem noch nicht veröffentlichte Sicherheitslücken in Software und Hardware ausgenutzt.[11]

9 http://www-03.ibm.com/press/de/de/pressrelease/42056.wss

10 http://nationalsecurityzone.org/war2-0/network/darpa/

11 Ein prominentes aktuelles Beispiel ist der sogenannte “Heartblead” Wurm. Hierbei handelt es sich um einen Sicherheitsfehler in der offenen SSL Verschlüsselungsbibliothek, die viele Webseiten und Internetdienste nutzen. http://heartbleed.com/ In der Presse wurde berichtet, dass die NSA diesen Sicherheitsfehler möglicherweise zur Informationsbeschaffung ausgenutzt hat. http://www.spiegel.de/netzwelt/netzpolitik/heartbleed-nsa-soll-sicherheitsluecke-seit-zwei-jahren-nutzen-a-964032.html

1.4 Technischen Fähigkeiten des BND

Dank der Enthüllungen von Edward Snowden sind wir in Deutschland in der paradoxen Lage, dass wir mehr über die technischen Fähigkeiten der amerikanischen und britischen Auslandsgeheimdienste als über die eigenen Nachrichtendienste wissen. Es ist allerdings naiv anzunehmen, dass die neuen Überwachungsmöglichkeiten, die mit der digitalen Revolution einhergehen, nicht auch vom BND für die strategische Aufklärung genutzt werden. Deutsche Dienste sind traditionell für ihre Stärken in der Fernmeldeaufklärung bekannt. Dies lässt sich zum einem auf das in Deutschland vorhandene technische Know-How zurückführen. Zum anderen kam gerade Deutschland während des Kalten Krieges aufgrund seiner geographischen Lage eine Schlüsselrolle bei der Überwachung des Fernmeldeverkehrs der Sowjetunion und des ehemaligen Ostblocks zu. Auch für deutsche Nachrichtendienste ist die Bekämpfung des internationalen Terrorismus zu einer zentralen Aufgabe geworden. Genauso haben sich für die deutschen Nachrichtendienste auch die Möglichkeiten der technischen Aufklärung aufgrund der Verbreitung von neuen Kommunikationstechnologien massiv ausgeweitet.

Es gibt eine Reihe von starken Indizien, die nahelegen, dass der BND seine technische Auslandsaufklärung auch entsprechend der neuen technologischen Möglichkeiten weiterentwickelt hat. Im Zuge der Enthüllungen von Edward Snowden wurde bekannt, dass der BND monatlich 500 Millionen Verbindungsdaten an die Vereinigten Staaten weitergibt.[12] Solche Datenmengen können nur mit großflächigen Überwachungsprogrammen, wie zum Beispiel der erwähnten Upstream-Methode, gewonnen werden. Hierfür gibt es in Deutschland exzellente Voraussetzungen. Schließlich befindet sich der weltweit größte Internetknoten in Frankfurt, über den ein erheblicher Anteil des globalen Internetverkehrs geroutet wird.[13] Aus den Berichten des parlamentarischen Kontrollgremiums an den Bundestag kann man auch entnehmen, dass der BND massenhaft Emails überwacht. So wurden 2010 allein im Gefahrenbereich „Proliferation“ 27 Millionen Emailverkehre zur weiteren Auswertung erfasst.[14] Eine so hohe Trefferzahl in einem so speziellen Gefahrengebiet ist allerdings nur vorstellbar, wenn dabei eine um ein Vielfaches höhere Anzahl an Emails auf die relevanten Suchbegriffe hin gescannt wurde.[15] Während es keine Zweifel gibt, dass der BND Upstream-Überwachung betreibt, ist eine Bewertung der technischen Fähigkeiten des BND in Bezug auf Downstream und spezielle Operationen nicht möglich, da hierüber kaum öffentlich zugängliche Informationen vorliegen und zum Beispiel die Dienstvorschriften zu informationstechnischen Operation als geheim eingestuft sind. Es ist allerdings anzunehmen, dass der BND hier auch dank Kooperationen mit NSA und GCHQ über größere Fähigkeiten verfügt, als in der Öffentlichkeit weithin angenommen wird.

Für die Geheimdienste haben sich mit dem technologischen Fortschritt der letzten Jahre ungeahnte Möglichkeiten für Überwachung und Spionage eröffnet. Die Enthüllungen von Edward Snowden haben hierüber eine längst überfällige, breite, gesellschaftspolitische Debatte ausgelöst. Schließlich ist in demokratischen Rechtsstaaten nicht alles erlaubt, nur weil es technisch möglich ist. Das gilt auch für die Geheimdienste. In den Vereinigten Staaten wie auch in Deutschland operieren Geheimdienste innerhalb eines vom Gesetzgeber definierten Rahmens, dessen Einhaltung von unabhängigen

12 http://www.sueddeutsche.de/politik/bnd-nsa-spaehaffaere-die-millionen-frage-1.1742027

13 Aus der Liste der Peering Partner am Internetknoten in Frankfurt wird deutlich, wie viele internationale Internetdienstleister sich dort zusammenschließen. https://www.de-cix.net/customers-partners/customers/de-cix-frankfurt/

14 Drucksache des Bundestages 17/8639, Seite 6.

15 Die Bundesregierung hat die hohe Trefferzahl mit einem ungewöhnlich hohen Spamaufkommen erklärt. Trotzdem ist die hohe Trefferzahl ein starkes Indiz, dass auch vom BND im großen Stil digitale Kommunikationsverkehre überwacht werden. Siehe http://www.heise.de/newsticker/meldung/Geheimdienste-ueberwachten-37-Millionen-Netzverbindungen-1442867.html

Kontrollinstitutionen gewährleistet werden soll. Die Grundzüge dieses rechtsstaatlichen Rahmens wurden auf beiden Seiten des Atlantiks während des Kalten Krieges definiert. Ob dieser rechtsstaatliche Rahmen allerdings angesichts der vor wenigen Jahren noch undenkbar erscheinenden technischen Aufklärungsmöglichkeiten immer noch angemessen ist, ist eine zentrale Frage, der man sich nicht nur in den Vereinigten Staaten, sondern auch in Deutschland dringend stellen muss.

2. Historischer Ursprung des rechtlichen Rahmens

Der rechtliche Rahmen für strategische Auslandsüberwachung wurde in der Bundesrepublik Deutschland im Kontext des Kalten Krieges geschaffen. Die damit verbundene Grundgesetzänderung liegt mittlerweile über 35 Jahre zurück. Sie bildete die Grundlage für die Einschränkung des Rechtsweges und das Instrument der parlamentarischen Kontrolle. Das Prinzip der parlamentarischen Kontrolle hat sich mittlerweile als zentrales Element der rechtsstaatlichen Grundlage, auf dessen Basis die deutschen Nachrichtendienste operieren, etabliert. Dabei wird leicht vergessen, dass die Einschränkung der Informationspflicht und die damit einhergehende Beschränkung des Rechtswegs ursprünglich äußerst kontrovers diskutiert wurden und dass für viele Kritiker ein vom Parlament beauftragtes Gremium kein adäquater Ersatz für gerichtliche Kontrolle sein konnte.[16]

2.1 Der steinige Weg zu den „Überwachungsgesetzen“

Um Überwachungsmaßnahmen von alliierten auf deutsche Nachrichtendienste übertragen zu können, mussten im Kalten Krieg zuerst die rechtlichen Voraussetzungen geschaffen werden. Schließlich handelte es sich bei den vorgesehenen Überwachungsmaßnahmen um schwere Grundrechtseingriffe, insbesondere Artikel 10 des Grundgesetzes. Das deutsche Grundgesetz schützt in Artikel 10 explizit die Kommunikation deutscher Bürger vor dem Zugriff Dritter einschließlich staatlicher Organe. In der Verfassung von 1949 wird das Brief-, Post- und Fernmeldegeheimnis als unverletzlich bezeichnet und damit als ein hohes Rechtsgut geschützt. Weiter heißt es, dass Beschränkungen nur im Rahmen eines Gesetzes angeordnet werden dürfen. Für geheimdienstliche Überwachung fehlte allerdings bis 1968 die ihm Grundgesetz verlangte gesetzliche Grundlage.

Ein sogenanntes „Überwachungsgesetz“ wurde in Deutschland seit den 1950er Jahren kontrovers diskutiert.[17] Die Alliierten drängten die deutsche Bundesregierung schon frühzeitig darauf, die Überwachung des Brief-, Post- und Fernmeldeverkehrs durch eigene Dienste zu übernehmen. Die Bundesregierung sah darin vor allem eine Chance, wichtige Souveränitätsrechte zurückzugewinnen. Die gesetzliche Umsetzung gestaltete sich allerdings als äußerst schwierig und es dauerte beinahe zwei Jahrzehnte, bis entsprechende rechtlichen Voraussetzungen mit einer Grundgesetzänderung und der Verabschiedung des G-10 Gesetzes geschaffen wurden. Besonders die Genehmigung und richterliche Überprüfung von Überwachungsmaßnahmen wurden äußerst kontrovers diskutiert. Experten bezweifelten, dass insbesondere breit angelegte Überwachungsprogramme ohne konkreten Anlassverdacht einer gerichtlichen Überprüfung standhalten würden.[18] Die Bundesregierung entschied sich letztendlich in ihrem Gesetzesentwurf für ein Genehmigungsverfahren innerhalb der zuständigen Ministerien anstatt einer Genehmigung durch eine mit Richtern besetzte Kommission. Das vorgelegte Gesetz schränkte auch den Rechtsweg zur Überprüfung von

16 Eine detaillierte Aufarbeitung der historischen Ursprünge des Rechtsrahmens deutscher Überwachungsbehörden und –Maßnahmen findet man in: Josef Foschepoth. (2013): Überwachtes Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik. Sonderausgabe für die Bundeszentrale für politische Bildung. (Göttingen: Vandenhoek &Ruprecht).

17 Foschepoth, S. 160

18 Foschepoth, S. 171

Überwachungsmaßnahmen ein. Stattdessen sollte ein vom Parlament eingesetztes Kontrollorgan die Überprüfung der geheimdienstlichen Überwachungsmaßnahmen vornehmen.

Die Ersetzung richterlicher Genehmigung und Kontrolle durch ein vom Parlament einzusetzendes Kontrollorgan bildeten den Grundpfeiler der Gesetzgebung von 1968. Artikel 10 des Grundgesetz wurde um den Zusatz erweitert, dass zum „Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes“ gesetzlich festgelegt werden kann, Eingriffe in das Brief-, Post- und Fernmeldegeheimnis betroffenen Personen nicht mitzuteilen. Ohne Mitteilung haben betroffene Personen allerdings so gut wie keine Möglichkeit die Rechtmäßigkeit des Grundrechtseingriffs auf dem Rechtsweg überprüfen zu lassen. Weiter bestimmt das Gesetz, dass „an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt,“ und verankert so das Prinzip der parlamentarischen Kontrolle im Grundgesetz.

Das ebenfalls 1968 verabschiedete G 10 Gesetz regelt die im Grundgesetz erwähnten Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses. Bei Anhaltspunkten für einen Verdacht auf Straftaten, die die Sicherheit der freiheitlich demokratischen Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes, einschließlich der in der Bundesrepublik stationierten NATO Truppen, bedrohten, konnten individuelle Überwachungsmaßnahmen gegen Einzelpersonen oder Gruppen angeordnet werden. Allgemeine strategische Überwachung war gerechtfertigt, wenn die „Sammlung von Nachrichten über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland rechtzeitig zu erkennen“. Das Gesetz führte weiter aus, dass der für Beschränkungsmaßnahmen zuständige Bundesminister in Abständen von höchstens sechs Monaten ein Gremium von fünf vom Bundestag zu bestimmende Personen zu unterrichten hat. Das Gremium konnte den Bundesminister dazu veranlassen, für unzulässig befundene Maßnahmen unverzüglich aufzuheben. Im Gegensatz zu im Zusammenhang der Gefahrenabwehr verhängten Überwachungsmaßnahmen erlaubte das G-10 Gesetz von 1968 Überwachungsmaßnahmen im Rahmen der Strafprozessordnung nur auf richterliche Anordnung.

2.2 Die Kontroverse um die „Überwachungsgesetze“

Die oben beschriebene Erweiterung von Artikel 10 des Grundgesetzes und das G-10 Gesetz wurden vor ihrer Verabschiedung im Bundestag kontrovers diskutiert. Die Opposition kritisierte vor allem den Ausschluss des Rechtsweges und die vage und damit weit auslegbaren Überwachungsbefugnisse. Die Gesetze waren so umstritten, dass sie nur in einem Paket mit den Notstandsgesetzen verabschiedet werden konnten. Der Historiker Joseph Foschepoth kann außer wahltaktischen Überlegungen keine Gründe für das Einschließen der Überwachungsgesetze in ein Gesetzespaket mit den Notstandsgesetzen erkennen, da es sich bei der Grundgesetzänderung von Artikel 10 und dem G-10 Gesetz gar nicht um Notstandsgesetze handelte.[19]

Nicht nur viele Abgeordnete und Staatsrechtler sondern auch die Regierungen einiger Bundesländer hielten die neuen Überwachungsgesetze für verfassungswidrig. Die hessische Landesregierung reichte ein Jahr nach der Gesetzesänderung am 29. September 1969 ein Normenkontrollverfahren beim Bundesverfassungsgericht in Karlsruhe ein, dem sich auch der Stadtstaat Bremen anschloss. Der Antrag wurde vor allem mit dem Ausschluss des Rechtsweges begründet, der nach Auffassung der hessischen Landesregierung nicht mit grundlegenden Verfassungsnormen wie der Gewaltenteilung und dem Rechtsstaatsprinzip vereinbar war. Das Bundesverfassungsgericht befand

19 Foschepoth, S. 178-9

in seinem Urteil vom 15. Dezember 1970 die Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses für verfassungskonform und stärkte damit den Staatsschutz als höherwertiges Rechtsgut gegenüber der damit verbundenen Einschränkung der Grundrechte.

Die Kritik der Opposition am mangelnden Rechtsschutz der von Überwachung betroffenen Bundesbürger blieb wirkungslos. Das Kalkül der Bundesregierung ging mit der Verabschiedung des Gesetzespakets auf. Jedoch konnte auch das Bundesverfassungsgericht die Kritik an der Grundgesetzänderung nicht beenden. Drei Richter gaben ein Minderheitsvotum ab, in dem sie die Geheimhaltung von Maßnahmen und den damit verbundenen Ausschluss des Rechtsweges für Betroffene als nicht mit dem Grundsatz der Menschenwürde vereinbar sahen. Nicht nur unter Verfassungsrichtern sondern auch unter Staatsrechtlern war die Grundgesetzänderung von 1968 äußerst umstritten, da es Staatsräson über Grundrechtsschutz stellte. Kritiker stieß vor allem auf, dass die Überwachungsmaßnahmen nicht nur Verdächtige, sondern generell jeden Bürger betreffen konnte, und kritisierten, dass parlamentarische Kontrolle den Rechtsweg niemals adäquat ersetzen könne.

Der Europäische Gerichtshof befasste sich 1978 mit der Grundgesetzänderung und erklärte die 1968 vorgenommenen Einschränkungen für vereinbar mit der Europäischen Menschenrechtskonvention und hierbei insbesondere mit dem Recht auf Privatheit (Artikel 8), dem Recht auf Beschwerde (Artikel 13) und dem Recht auf ein faires Verfahren (Artikel 6). Auch hier wurde von den Richtern vorausgesetzt, dass Beschränkungsmaßnahmen grundsätzlich regelkonform und unter strenger Kontrolle durchgeführt wurden. Es verknüpfte die Rechtmäßigkeit der Maßnahmen allerdings mit drei Punkten: dem Vorliegen eines Anfangsverdachts, Notwendigkeit von Benachrichtigungen Betroffener, um zumindest nachträgliche Gerichtsüberprüfungen zu ermöglichen, und die Beschränkung der Maßnahmen auf Einzelpersonen. Mit allgemeiner Überwachung im Sinne der strategischen Auslandsaufklärung befassten sich die Richter in ihrem Urteil gar nicht.

3. Rechtliche Rahmen heute

Seit der ersten Fassung von 1968 ist das Gesetz vor allem um detaillierte Vorgaben zur Beantragung und Durchführung von Überwachungsmaßnahmen des Telekommunikations- und Postverkehrs erweitert worden. Paragraph 2 des Gesetzes verpflichtet die Telekommunikationsanbieter zur Kooperation. Auf Anweisung haben Telekommunikationsunternehmen staatlichen Behörden die zur Überwachung notwendigen Schnittstellen zur Verfügung zu stellen. Das G-10 Gesetz unterscheidet grundsätzlich zwischen Beschränkungen in Einzelfällen (Abschnitt 2) und strategischen Beschränkungen (Abschnitt 3), die im Mittelpunkt unseres Interesses stehen. Bei Beschränkungen in Einzelfällen, oft auch als Individualmaßnahmen bezeichnet, müssen „tatsächliche Anhaltspunkte für den Verdacht“ bestehen, dass Einzeltäter oder Gruppen in Paragraph 3 aufgelistete Straftaten begehen könnten. Darunter fallen unter anderem Friedensverrat, Hochverrat und Landesverrat. Allerdings kritisiert der Staatsrechtler Matthias Bäcker in seiner Stellungnahme für den NSA Untersuchungsausschuss des Bundestags die Ermächtigungen für Individualmaßnahmen als so weit gefasst, dass sie „Telekommunikationsüberwachungen bereits in eher diffusen Bedrohungslagen von teils nur geringem Gewicht“ ermöglichen.[20]

Neben individuellen Überwachungsmaßnahmen erlaubt Paragraph 5 des G-10 Gesetzes auch sogenannte strategische Beschränkungen. Hierbei werden internationale Telekommunikationsverkehrsströme mit Hilfe von Suchbegriffen überwacht. Strategische Überwachungsmaßnahmen dürfen

20 Bäcker, Matthias (2014): Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhörung des NSA Untersuchungsausschusses am 22. Mai, 2014, S. 5

für eine ganze Reihe von verschiedenen Sachverhalten wie z. B. der Erfassung von Informationen zu bewaffneten Angriffen auf die Bundesrepublik Deutschland, dem Begehen internationaler terroristischer Anschlägen, der internationalen Verbreitung von Kriegswaffen, Drogenhandel, organisierte Kriminalität oder internationaler Geldwäsche angewendet werden. Auch hier sieht der Staatsrechtler Matthias Bäcker Handlungsbedarf, da den neuen technischen Möglichkeiten durch die Gesetzgebung kaum wirksame Grenzen gesetzt werden. Nach seiner Einschätzung lässt das Gesetz „Auslegungen zu, die auf eine annähernd vollständige Erhebung des Telekommunikationsverkehrs mit bestimmten ausländischen Staaten und eine weitreichende Erhebung auch des inländischen Telekommunikationsverkehrs hinauslaufen."[21] So lässt sich zum Beispiel die Einschränkung strategischer Maßnahmen auf internationale Telekommunikationsverkehre in der Praxis gar nicht umsetzen, da auch viele innerdeutsche Telekommunikationsverkehre über internationale Verbindungen laufen. Auch die Einschränkung der zu nutzenden Übertragungskapazität lässt sich nicht wirksam umsetzen. Auf diesen Punkt werden wir im weiteren Verlauf noch mehrfach zurückkommen.

3.1 Beantragung der Überwachungsmaßnahmen

Das G-10 Gesetz schreibt für die nach diesem Gesetz durchgeführten Überwachungsmaßnahmen der Nachrichtendienste des Bundes eine Antragsstellung (Abschnitt 4) vor. So muss der BND Überwachungsmaßnahmen bei der für die Nachrichtendienste zuständigen Abteilung 6 des Bundeskanzleramts schriftlich beantragen und begründen. Bei Individualmaßnahmen muss die zu überwachende Person oder Personengruppe benannt und dargelegt werden, dass die „Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert" wäre. Bei strategischen Maßnahmen nach Paragraph 5 müssen die Suchbegriffe in der Anordnung aufgeführt werden. Des Weiteren müssen das geographische Gebiet und die zu überwachenden Übertragungswege benannt werden. Das Gesetz sieht dabei vor, dass nicht mehr als 20% der auf dem Übertragungsweg zur Verfügung stehenden Übertragungskapazität überwacht werden darf. Die genehmigten Anträge gelten jeweils für drei Monate und können jeweils um maximal drei Monate verlängert werden.

Des Weiteren enthält das G-10 Gesetz Bestimmungen zum besonderen Schutz zeugnisverweigerungsberechtigter Personen und zur Prüfung, Kennzeichnung, Löschung, Übermittlung und Zweckbindung von erhobenen Daten. Gemäß Paragraph 7 kann das Bundeskanzleramt eine Übermittlung von Daten an ausländische Dienste genehmigen, wenn außen- und sicherheitspolitische Interessen Deutschlands betroffen sind und die Verwendung der Daten mit rechtsstaatlichen Prinzipien in Einklang steht. Nach Beendigung einer Individualmaßnahme schreibt das Gesetz eine Benachrichtigung der betroffenen Personen vor. Auf eine Benachrichtigung kann verzichtet werden, wenn eine „Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar" ist. Über Anträge der Dienste, Benachrichtigungen aus diesen Gründen zurückzustellen, entscheidet die G-10 Kommission.

3.2 Die Rolle der G-10 Kommission

Das G-10 Gesetz regelt auch die Grundlagen der Tätigkeiten der sogenannten G-10 Kommission, deren Aufgabe es ist, über die Zulässigkeit und Notwendigkeit der von den Ministerien genehmigten Überwachungsmaßnahmen zu entscheiden. Der Aufgabenbereich der Kommission erstreckt sich auf die „gesamte Erhebung, Verarbeitung und Nutzung der nach diesem Gesetz erlangten personenbezogenen Daten durch Nachrichtendienste des Bundes einschließlich der Entscheidung über die Mitteilung an Betrof-

21 Bäcker, S. 9

fene." Die Kommission bestehend aus einem Vorsitzenden, der über die Befähigung zum Richteramt verfügen muss, drei Beisitzern und vier stellvertretenden Mitgliedern und wird vom Parlamentarischen Kontrollgremium eingesetzt. Die Kommission tritt monatlich zu geheimen Beratungen zusammen. Laut G-10 Gesetz kann die G-10 Kommission zur Wahrnehmung ihrer Kontrolltätigkeit Fragen an die Nachrichtendienste richten und Einsicht in ihre Unterlagen nehmen. Zur Erfüllung ihrer Aufgaben sind der Kommission die notwendige Sach- und Personalausstattung und dabei explizit auch Mitarbeiter mit technischem Sachverstand zur Verfügung zu stellen.

3.3 Die Rolle des Parlamentarischen Kontrollgremiums

Das Gesetz zur parlamentarischen Kontrolle nachrichtendienstlicher Tätigkeit aus dem Jahr 2009 verlangt, dass der Bundestag in jeder Legislaturperiode ein spezielles Gremium aus Abgeordneten einsetzt. Die Bundesregierung ist verpflichtet dieses Gremium mindestens einmal vierteljährlich über die „allgemeinen Tätigkeiten" der Nachrichtendienste sowie „besondere Vorgänge" zu unterrichten. Laut Paragraph 5 des G-10 Gesetzes bedürfen strategische Überwachungsmaßnahmen internationaler Telekommunikationsbeziehungen der Zustimmung des parlamentarischen Kontrollgremiums. Die Bundesregierung hat auf Nachfragen aus dem parlamentarischen Kontrollgremium Auskunft zu geben und gegebenenfalls Einsicht in Akten und gespeicherte Daten zu gewähren. Das Gremium kann Mitarbeiter der Dienste befragen, die verpflichtet sind, vollständige und wahrheitsgemäße Angaben zu machen. Die Bundesregierung kann allerdings die Auskunft verweigern, wenn dies „aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist oder wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist." Zusätzlich ist die Auskunftspflicht auf Gegenstände beschränkt, die der Verfügungsberechtigung der deutschen Nachrichtendienste unterliegen. Deutsche Dienste haben in der Regel keine Verfügungsberechtigung über von ausländischen Partnern zur Verfügung gestellte Informationen.

Das parlamentarische Kontrollgremium kann mit einer Zweidrittelmehrheit beschließen, Sachverständige mit der weiteren Prüfung eines im Gremium bereits diskutierten Sachverhalts zu beauftragen. Das Gremium tagt geheim. Mit einer Zweidrittelmehrheit kann der Geheimschutz für eine Bewertung des Gremiums allerdings aufgehoben werden. Eine Zweidrittelmehrheit ermöglicht es auch, die Ergebnisse eigener Untersuchungen öffentlich an den Bundestag zu übermitteln. Mitarbeiter der Gremiumsmitglieder können unter Einhaltung des Geheimschutzes Zugang zu Akten und Dateien bekommen. Sie dürfen jedoch nicht an den Sitzungen des Gremiums teilnehmen. Ferner bestimmt das Gesetz, dass das Gremium dem Bundestag mindestens zur Mitte und zum Ende der Wahlperiode einen Bericht über seine Kontrolltätigkeit vorzulegen hat.

Die untenstehende Tabelle fasst die wesentlichen Kontrollaufgaben und Kontrollbefugnisse der G-10 Kommission und des Parlamentarischen Kontrollgremiums in Bezug auf die Telekommunikationsüberwachung bundesdeutscher Nachrichtendienste zusammen.

Tabelle 1 Unabhängige Kontrolle über die Telekommunikationsüberwachung des BNDs

	G-10 Kommission	Parlamentarisches Kontrollgremium
Kontrollmandat	Personenbezogene Beschränkungsmaßnahmen	Regierungsführung in Bezug auf die allgemeine Tätigkeit der Nachrichtendienste des Bundes, inklusive der strategischen Beschränkungsmaßnahmen[1]
Kontrollbefugnis	Entscheidet über Zulässigkeit und Notwendigkeit von personenbezogenen Beschränkungsmaßnahmen	Wird über alle Anordnungen von Beschränkungsmaßnahmen informiert. Laut G-10 Gesetz Zustimmung zu strategischen Beschränkungen internationaler Telekommunikationsbeziehungen und der Geschäftsordnung der G-10 Kommission
Berichtspflichten	Keine; Gibt sich selbst eine Geschäftsordnung	Jährlicher Bericht an den Bundestag über Durchführung, Art und Umfang der Beschränkungsmaßnahmen[2]
Sitzungen	Ein Mal pro Monat unter Ausschluss der Öffentlichkeit	Mindestens 4 Mal im Jahr unter Ausschluss der Öffentlichkeit
Mitglieder	Vier Mitglieder, vier Stellvertreter	Neun Mitglieder

3.4 Durchführung und Kontrolle der Überwachungsmaßnahmen

Der Schwerpunkt der Kontrolle der Überwachungsmaßnahmen liegt bei den Diensten und den sie beaufsichtigenden Ministerien. Die genehmigten Überwachungsmaßnahmen sind gemäß Paragraph 11 des G-10 Gesetzes unter Aufsicht eines Bediensteten vorzunehmen, der die Befähigung zum Richteramt hat. Die Behörde hat die Maßnahme unverzüglich zu beenden, wenn die „Voraussetzungen der Anordnung“ nicht mehr gegeben sind oder die Maßnahme schlicht nicht mehr erforderlich ist. Die G-10 Kommission nimmt als unabhängige Kontrollinstanz hierbei eine Schlüsselrolle ein. Wie weiter unten noch ausgeführt wird, ist ihre Kontrolltätigkeit allerdings auf Überwachungsmaßnahmen mit Deutschlandbezug beschränkt. Das heißt, die G-10 Kommission prüft nur die Genehmigung von Maßnahmen, die deutsche Staatsbürger betreffen oder bei denen Kommunikationsverkehre entweder einen Ausgangs- oder einen Endpunkt in Deutschland haben. Strategische Maßnahmen nach Paragraph 5 bedürfen laut G-10 Gesetz der Zustimmung des parlamentarischen Kontrollgremiums.
Allerdings vertritt die Bundesregierung die Auffassung, dass das G-10 Gesetz nicht für die strategische Fernaufklärung gilt, wenn weder Anfang noch Ende der Kommunikationsverbindung in Deutschland sind. Somit findet die strategische Auslandsaufklärung ohne die Beschränkungen des G-10 Gesetzes statt.

3.5 Die Bedeutung territorialer Bezüge

Bertold Huber und Johannes Caspar haben jüngst in juristischen Fachartikeln darauf hingewiesen, dass für die rechtliche Einordnung der Befugnisse und Kontrolle der Nachrichtendienste territoriale Bezüge von elementarer Bedeutung sind.[22] Im Kern handelt es dabei um die von Bertold Huber in seinem Artikel aufgeworfene Frage, ob das Grundgesetz auch außerhalb des deutschen Staatsgebiets gilt. Da das G-10 Gesetz den gesetzlichen Rahmen für Eingriffe in das in Artikel 10 des Grundgesetzes festgeschriebene Brief-, Post- und Fernmeldegeheimnis festschreibt, kann man logisch folgern, dass das G-10 Gesetz nicht bei Fällen zur Anwendung kommen kann, die gar keinen Eingriff in Artikel 10 darstellen. Laut Bertold Huber, der selbst seit 1997 der G-10 Kommission angehört, rechtfertigt die Bundesregierung ihre Haltung, dass die G-10 Kommission nicht für Fälle der Ausland-Ausland Überwachung zuständig ist mit der Behauptung, dass bei der strategischen Auslandsaufklärung keine unmittelbaren territorialen oder technischen Bezüge zur Bundesrepublik Deutschland bestünden.[23]

Gemäß dieser territorialen Differenzierung sind bei der rechtliche Einordnung von Überwachungsmaßnamen grundsätzlich drei Formen von Telekommunikationsverkehren hinsichtlich ihrer geographischen Beziehungen zu unterscheiden: Inland-Inland, Inland-Ausland und Ausland-Ausland.[24] Kommunikationsverkehre innerhalb von Deutschland (Inland-Inland), bei der sich beide Telekommunikationsteilnehmer in Deutschland befinden, gehören nicht zur strategischen Auslandsüberwachung und dürfen generell nicht vom BND überwacht werden. Kommunikationsbeziehungen zwischen Deutschland und dem Ausland (Inland-Ausland) fallen unter das G-10 Gesetz und damit auch in den Kompetenzbereich der G-10 Kommission. Die eigentliche Kernaufgabe des BND, nämlich die Überwachung von Kommunikationsverkehren von Ausländern im Ausland (Ausland-Ausland), stellt dieser territorialen Logik zufolge keinen Eingriff in Artikel 10 des Grundgesetzes dar und wird daher auch gar nicht vom G-10 Gesetz erfasst. Das Argument, dass Ausland-Ausland Überwachung gar nicht vom G-10 Gesetz erfasst wird, wird noch zusätzlich durch die Definition von internationalen Telekommunikationsverkehren als „Telekommunikationsbeziehungen, die von oder nach Deutschland geführt werden“ gestützt.[25] Telekommunikationsbeziehungen ohne territorialen Bezug zu Deutschland werden demzufolge überhaupt nicht vom G-10 Gesetz behandelt.

3.6 Kontrollvakuum in der strategische Auslandsaufklärung

Die G-10 Kommission prüft die Zulässigkeit und Notwendigkeit von Eingriffen in das im Artikel 10 des Grundgesetz festgeschriebenen Brief-, Post- und Fernmeldegeheimnis. Die Bundesregierung vertritt die Meinung, dass diese Kontrollfunktion sich nicht auf die sogenannte strategische Auslandsüberwachung bezieht, da es bei der Überwachung von Kommunikationsverkehren mit „Ausgangs- und Endpunkt jeweils im Ausland keinen unmittelbaren territorialen oder technischen Bezug (mit Ausnahme der Datenverarbeitung) zur Bundesrepublik Deutschland“ gebe.[26] Das Bundesverfassungsgericht hat allerdings in einem Urteil im Jahr 1999 festgestellt, dass die Grundrechte nicht territorial, sondern an die Ausübung staatlichen Handelns gebunden sind. Daraus lässt sich ableiten, dass auch Überwachungsmaßnahmen, die Ausländer im Ausland betreffen, Grundrechtseingrif-

22 Huber, Bertold (2013): Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite. Neue Juristische Wochenschrift, Heft 35/2013, S.2572-2577; Caspar, Johannes (2014): Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats? Privacy in Germany, Heft 1/2014, S. 1-6.

23 Siehe dazu auch Bäcker, S. 16-22.

24 Caspar, Seite 2.

25 Huber, Seite 2573, Fußnote 8

26 Huber, Seite 2575.

fe im Sinne von Artikel 10 sind.[27] Bertold Huber argumentiert in Berufung auf dieses Urteil des Bundesverfassungsgerichts, dass daher auch die Anordnungen zur strategischen Auslandsüberwachung von der G-10 Kommission überprüft werden müssten. Das Bundesverfassungsgericht hat allerdings über die Frage, ob die Überwachung von Ausland-Ausland Verkehren auch dem G-10 Gesetz unterliegt im Verfahren von 1999 nicht geurteilt.

Wenn die G-10 Kommission allerdings nicht zuständig ist, bleibt nur noch die mögliche Kontrolle durch das parlamentarische Kontrollgremium. In diesem Kontext ist es wichtig hervorzuheben, dass parlamentarische Kontrolle nicht mit den Kontrollbefugnissen der G-10 Kommission gleichzusetzen ist.[28] Das parlamentarische Kontrollgremium hat im Unterschied zur G-10 Kommission nicht über Zulässigkeit und Notwendigkeit von Überwachungsmaßnahmen zu entscheiden. Auch die größeren Zeitabstände zwischen den Sitzungen verknüpft mit einem breiteren Mandat und der Politisierung des Gremiums führen dazu, dass Kontrolle durch das parlamentarische Kontrollgremium qualitativ nicht mit Kontrolle durch die G-10 Kommission gleichzusetzen ist. Dieser Punkt wird im nächsten Kapitel noch ausführlicher diskutiert.

3.6 Fazit: rechtlicher Rahmen muss dringend reformiert werden

Die zuletzt behandelte Frage nach dem Geltungsbereich des G-10 Gesetzes wirft bereits eines der entscheidenden Probleme in Bezug auf den rechtlichen Rahmen für die vom BND durchgeführte strategische Auslandsüberwachung auf. Die Unterscheidung zwischen In- und Ausland und eigenen Staatsbürgern und Ausländern ist eben nicht nur ein Kernelement der amerikanischen Überwachungspraxis. Sie findet sich auch in Deutschland wieder. Sie ist allerdings nicht auf den ersten Blick erkennbar, da die Bedeutung der Unterscheidung zwischen In- und Ausland und Staatsbürgern und Ausländern sich nicht aus dem Gesetzestext selbst, sondern erst in Bezug auf den Geltungsbereich des Grundgesetzes erschließt.

Diese von der Bundesregierung vorgenommene Unterscheidung ist nicht mit der deutschen Verfassung vereinbar, wenn man der Argumentation von Bertold Huber und weiteren prominenten deutschen Staatsrechtlern folgt, dass Grundrechte nicht territorial, sondern an die Ausübung von Staatsgewalt gebunden sind. Wenn Grundrechtsschutz den Staat auch bei seinen extraterritorialen Aktivitäten bindet, ist die Einschränkung des Mandats der G-10 Kommission auf deutsche Staatsbürger und deutsches Staatsgebiet nicht mit der Verfassung vereinbar. Neben dem Problem, dass unsere Nachrichtendienste in den Augen prominenter Staatsrechtler außerhalb der Verfassung operieren, bringt diese Unterscheidung auch ein Glaubwürdigkeitsproblem mit sich. Es ist schwierig, die Regierung der Vereinigten Staaten von Amerika für die Differenzierung zwischen Ausländern und Staatsangehörigen beim Schutz vor Überwachung zu kritisieren, wenn die deutsche Regierung selbst für diese Differenzierung in Bezug auf die Tätigkeiten der eigenen Nachrichtendienste eintritt. Wie wir im nächsten Kapitel darlegen, greift auch eine Ausdehnung der Kompetenzen der G-10 Kommission und des parlamentarischen Kontrollgremiums auf den Bereich der strategischen Auslandsaufklärung ohne Deutschlandbezug zu kurz. Denn wie wir im folgenden Kapitel darlegen, haben wir nicht nur ein Problem mit den rechtlichen Grundlagen sondern auch mit der Kontrolle

27 Diese Auffassung wird auch von den Staatsrechtlern Matthias Bäcker, Hans-Jürgen Papier und Wolfgang Hoffmann-Riem in ihren Stellungnahmen für den parlamentarischen Untersuchungsausschuss (NSA) vertreten. http://www.bundestag.de/presse/pressemitteilungen/2014/pm_1405157/279268

28 Unter demokratietheoretischen Aspekten scheint es äußerst fragwürdig, dass das Parlament überhaupt eine Befugnis zur Kontrolle benötigt. Eigentlich müsste es andersherum sein. In einer Demokratie wäre zu erwarten, dass sich die mittelbar legitimierten Behörden bzw. die Bundesregierung beim unmittelbar legitimierten Parlament die Befugnis einholen müssten, einen Teil der nachrichtendienstlichen Tätigkeiten nicht der Kontrolle zu unterwerfen.

technischer Überwachung.

Neben der aus der Perspektive des Grundgesetzes problematischen Unterscheidung zwischen In- und Ausländern kommt noch hinzu, dass bei über das Internet stattfindenden Kommunikationsverkehren die klare Unterscheidung zwischen in- und ausländischen Kommunikationsverkehren in der Praxis kaum möglich ist. Internetverkehr wird global geroutet. Davon profitiert der BND, da der Dienst dadurch am Internetknoten in Frankfurt auch Zugang zu Kommunikationsverkehren mit Anfangs- und Endpunkt im Ausland erhält. Gleichzeitig werden aber auch eine große Zahl von Kommunikations- und Datenverkehren zwischen deutschen Bürgern in Deutschland über das Ausland geroutet.[29] Der BND verfügt über keine rechtlichen Befugnisse auf diese Kommunikationsverkehre zuzugreifen. Technisch ist es allerdings aufgrund der globalen Infrastrukturen unmöglich auszuschließen, dass im Rahmen der technischen Auslandsaufklärung nicht auch innerdeutsche Kommunikationsverkehre in den Fokus des BND geraten.

Wie dieses Beispiel zeigt, stellt technologischer Fortschritt unsere rechtlichen Konzepte und Normen und deren Anwendbarkeit auf die strategische Auslandsüberwachung zunehmend in Frage. Kapitel 1 hat eine ganze Reihe von neuen Methoden skizziert, die die technischen Überwachungsmöglichkeiten massiv ausgeweitet haben und zugleich nicht mit den gesetzlich festgeschriebenen Begrenzungen zu fassen sind. So schreibt das G-10 Gesetz zum Beispiel vor, dass bei strategischen Überwachungen auf nicht mehr als 20% der auf den Übertragungswegen zur Verfügung stehenden Übertragungskapazität zugegriffen werden darf. Angesichts der Behauptung der NSA auf nicht mehr als 1,6% des globalen Internet Verkehrs Zugriff zu haben, wurde aber bereits von Experten darauf hingewiesen, dass, wenn man die sehr datenintensiven Unterhaltungsanwendungen ausklammert, die NSA wirklich nur an etwa 3% des globalen Internetverkehrs interessiert sei.[30] In der Praxis dürfte die Einschränkung auf 20% der Übertragungskapazität bei der Überwachung des Internetverkehrs für den BND daher gar keine Rolle spielen.

Das G-10 Gesetz enthält mit Paragraph 3a eine eigene Klausel zum besonderen Schutz des Kernbereichs privater Lebensführung. Werden zum Beispiel in überwachten Gesprächen Themen, die den Kernbereich privater Lebensführung betreffen, angesprochen, ist die Maßnahme unverzüglich zu unterbrechen. Bestehen Zweifel, ob der Kernbereich privater Lebensführung betroffen ist, darf nur automatisch aufgezeichnet werden und die G-10 Kommission hat anschließend über die Verwertbarkeit der Daten zu entscheiden. Wie bereits in Kapitel 1 beschrieben wurde, ist der technologische Fortschritt in den letzten Jahren zunehmend in die Kernbereiche privater Lebensführung eingedrungen. Selbst die Auswertung von Verbindungsdaten erlaubt mittlerweile detaillierte Einblicke in intimste private Vorlieben und Verhaltensweisen.[31] Bei der strategischen Auslandsüberwachung kann auf riesige Mengen an sehr persönlichen Daten zugegriffen werden. Insbesondere wenn diese in großem Stil gesammelt und ausgewertet werden, ermöglichen sie die Erstellung von sehr genauen Kommunikations- und Verhaltensprofilen. Hier steht der Gesetzgeber vor der großen Herausforderung, durch geeignete gesetzliche Vorschriften dafür Sorge zu tragen, dass der besonders schützenswerten Kernbereich privater Lebensführung nicht durch technologische Entwicklungen in der geheimdienstlichen Praxis ausgehöhlt wird.

29 So führt zum Beispiel die Entscheidung der Telekom, nicht am Internetknoten DE-CIX in Frankfurt Daten mit anderen Netzbetreibern auszutauschen dazu, dass ein großer Anteil der Telekomdatenpakete aus innerdeutschen Verbindungen über das Ausland geroutet wird und damit auch in das Visier des BND geraten könnte. http://www.heise.de/netze/meldung/Das-DE-CIX-und-das-Schland-Netz-Betreiber-empoert-ueber-Telekom-Plaene-zum-Schengen-Routing-2044731.html

30 http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance

31 http://t3n.de/news/metadaten-brisant-stanford-studie-534512/

Ursprünglich richtete sich die Kritik an den „Überwachungsgesetzen“ hauptsächlich gegen die Einschränkung richterlicher Kontrolle zu Gunsten des Instruments der parlamentarischen Kontrolle. Aber auch in Bezug auf den rechtlichen Rahmen ist festzuhalten, dass der BND über weite Befugnisse zur strategischen Auslandsaufklärung verfügt. Gerade in diesem Bereich ist die Kontrolle durch unabhängige Gremien allerdings auch am schwächsten. Dies liegt vor allem an der territorialen Logik, die der Grundrechtsschutz bei Überwachungsmaßnahmen auch in Deutschland unterworfen ist. Überwachungsmaßnahmen durch den BND gegen deutsche Staatsbürger bedürfen der Genehmigung der von der Exekutive unabhängigen G 10 Kommission. Dieses Genehmigungsverfahren ist allerdings nicht bei der Überwachung von Ausländern im Ausland notwendig. Hier müsste eigentlich das parlamentarische Kontrollgremium tätig werden. Ein klares Mandat hierzu gibt es aufgrund der territorialen Logik des rechtlichen Rahmens aber nicht. Und auch die Praxis der parlamentarischen Kontrolle, das Thema des folgenden Kapitals, deutet darauf hin, dass die strategische Auslandsüberwachung des BND quasi ohne Kontrolle durch von der Exekutive unabhängige Institutionen sattfindet.

4. Analyse und Bewertung der parlamentarischen Kontrollpraxis

Im vorherigen Kapitel wurde bereits auf das Problem hingewiesen, dass die G-10 Kommission keine Kontrollkompetenz über strategische Auslandsaufklärung hat. Das parlamentarische Kontrollgremium kann dieses Vakuum nicht ausfüllen, da es im Gegensatz zur G-10 Kommission keine Entscheidungsbefugnis bezüglich einzelner Überwachungsmaßnahmen hat. Der G-10 Kommission müssen alle Überwachungsmaßnahmen, die unter das G-10 Gesetz fallen, zur Genehmigung vorgelegt werden. Dem parlamentarischen Kontrollgremium gegenüber ist die Bundesregierung laut dem Gesetz nur zur Unterrichtung über allgemeine Tätigkeiten und besondere Vorkommnisse verpflichtet – sie muss dem Gremium keine einzelnen Überwachungsmaßnahmen zur Genehmigung vorlegen.

4.1 Tätigkeitsberichte: In Pullach nichts Neues?

Die neun Mitglieder des parlamentarischen Kontrollgremiums kommen häufiger als die per Gesetz vorgeschriebenen vier Sitzungen im Jahr zusammen. Unter Ausschluss der Öffentlichkeit, aber in Gegenwart hoher Entscheidungsträger der Nachrichtendienste, des Kanzleramts und der Bundesministerien, kann in den Sitzungen des Gremiums das gesamte Spektrum nachrichtendienstlichen Handelns zur Sprache kommen. Seit 2011 beschließt das parlamentarische Kontrollgremium jährlich ein Arbeitsprogramm, um einzelne, wechselnde Themenbereiche „einer vertieften strukturellen und systematischeren“ Kontrolle zu unterwerfen.[32] Dies klingt vielversprechend, ist aber angesichts der Tatsache, dass den 10.500 Nachrichtendienstlern des Bundes (Bundesnachrichtendienst, Bundesverfassungsschutz und Militärischer Abschirmdienst) weniger als ein Dutzend Kontrolleure gegenüber steht, ein hochgestecktes Ziel.

Das parlamentarische Kontrollgremium hat dem Bundestag jährlich über Durchführung, Art und Umfang sämtlicher im G-10 Gesetz erwähnten Beschränkungsmaßnahmen zu berichten und darüber hinaus alle zwei Jahre einen Bericht über seine Kontrolltätigkeit im Allgemeinen zu verfassen. Diese Berichte stellen eine der wenigen öffentlich einsehbaren Informationsquellen zur Arbeit der parlamentarischen Kontrolle dar. Ein genaueres Studium der letzten drei Berichte über die Durchführung der von den Bundesministerien angeordneten Beschränkungsmaßnahmen des G-10 Gesetzes lässt erkennen, dass sich die Kontrolleure des Gremiums eher routinemäßig mit der Fern-

32 Drucksache des Bundestages 18/217, S. 3.

meldeaufklärung auseinandergesetzt haben und sich dabei mitunter eher als Berater der Nachrichtendienste verstanden haben, als als deren Kontrolleure.[33]

Dieser Eindruck entsteht zum einen, da die Berichte in der Regel mit einer Verspätung von über einem Jahr veröffentlicht werden. So erschien beispielsweise der Bericht für das Jahr 2011 im März 2013. In der Politik ist dieser Zeitunterschied erheblich und einer wirksamen Kontrolle abträglich. Die Bundestagsabgeordneten und die breite Öffentlichkeit zeigen erfahrungsgemäß wenig Interesse für Sachverhalte, die bereits über ein Jahr zurückliegen. Hier sollte der öffentliche Druck auf die Kontrolleure erhöht werden, die Jahresberichte zügiger nach Ende des Berichtszeitraums – vielleicht sogar innerhalb einer bestimmten Frist – zu veröffentlichen.

Desweiteren ist erstaunlich, wie spärlich das parlamentarische Kontrollgremium über seine eigenständige Kontrolltätigkeit in den jeweiligen Jahresberichten bekanntgibt. Schaut man sich die Drucksachen 18/218, 17/12773 und 17/8639 näher an, so erfährt man vergleichsweise wenig über die Jahresleistung des Gremiums auf diesem so wichtigen Gebiet. Die Berichte sind sehr knapp gehalten (Umfang unter 10 Seiten) und der Großteil eines jeden Berichttextes ist im Wortlaut nahezu identisch mit dem Bericht des Vorjahres. Die Dokumente erläutern zuerst die gesetzlichen Grundlagen (Grundlagen für die Berichtsplicht; das G-10 Gesetz; die G-10 Kommission und das Parlamentarische Kontrollgremium; Voraussetzungen für die personenbezogenen und strategischen Beschränkungsmaßnahmen) und berichten dann über die personenbezogenen Beschränkungsmaßnahmen, die der quasi-richterlichen Kontrolle der G-10 Kommission unterliegen.

Bis zum Abschnitt IV.2 „Art und Umfang der (strategischen) Beschränkungsmaßnahmen“ – am Ende der Berichte enthalten mehrere Überschriften bereits das Wort „Kontrolle“, ohne dass der Leser etwas darüber erfahren hat, wie genau das parlamentarische Kontrollgremium tätig geworden ist. Im Abschnitt, der die strategischen Beschränkungsmaßnahmen thematisiert, wird nur aufgezählt, mit wie vielen Suchbegriffen der BND in den drei mit Zustimmung der G-10 Kommission festgelegten Gefahrenbereichen „Internationaler Terrorismus“, „Proliferation und konventionelle Rüstung“ und „illegale Schleusung“ Telekommunikationsdaten nach Maßgabe von Paragraph 5 des G-10 Gesetzes erfasst hat. Zudem wird darüber informiert, wie viele der erfassten Telekommunikationsverkehre sich für einen Gefahrenbereich qualifiziert haben. Zum Beispiel wurde im ersten Halbjahr des Jahres 2012 im Gefahrenbereich „Internationaler Terrorismus“ mit 1088 formalen und 76 inhaltlichen Suchbegriffen eine unbekannte Zahl von Telekommunikationsverkehren erfasst. Auf das Jahr 2012 verteilt haben sich von der unbekannten Zahl der erfassten Telekommunikationsdaten 1804 Telekommunikationsverkehre für den Gefahrenbereich „internationaler Terrorismus“ qualifiziert. Der Bericht stellt auch fest, wie sich diese qualifizierten Telekommunikationsverkehre in E-Mail-Erfassung; Faxerfassung und SMS-Nachrichten aufteilen.

Ferner informieren die Jahresberichte knapp über die Praxis der gesetzlich vorgeschriebenen Mitteilungen an die Betroffenen von Beschränkungsmaßnahmen (eine Kompetenz der G-10 Kommission) und noch knapper über die vereinzelten strategischen Beschränkungsmaßnahmen zur Erkennung einer im Einzelfall bestehenden Gefahr für deutsche Staatsbürger im Ausland (fünf im Zeitraum 2012) sowie über die Häufigkeit und Art von Übermittlungen von Daten des BNDs an ausländische Partner im Rahmen einer bestimmten strategischen Beschränkungsmaßnahme nach Paragraph 5 des G-10 Gesetzes.

33 Die jüngsten öffentlich einsehbaren Berichte (Drucksachen des Bundestages 17/8639; 17/12773 und 18/218) decken den Zeitraum vom 01.01.2010 bis zum 31.12.2012 ab.

Was bei der Berichterstattung gänzlich fehlt, ist eine kritische Distanz zum Berichtsgegenstand sowie eine eigene Stimme des Kontrollorgans. Es ist verständlich, dass das parlamentarische Kontrollgremium Angaben der G-10 Kommission in seinem Jahresbericht aufführt, da diese Kommission keine eigenständige Berichtspflicht hat. Wenn das Kontrollgremium aber darüber hinaus auf die strategischen Beschränkungsmaßnahmen des BNDs zu sprechen kommt, so gibt es eigentlich nur die Angaben der Bundesministerien an den Bundestag weiter. Wenn dies das Ziel der „Kontrolle" wäre, könnte die Bundesregierung diese Informationen auch direkt und ohne Verzögerung an den Bundestag weitergeben. Das parlamentarische Kontrollgremium ist aber ein im Grundgesetz aufgeführtes Kontrollorgan (Artikel 45 des Grundgesetzes) und nicht die „Entgegennahme- und Weitergabestelle" von Regierungsinformationen.

In den Jahresberichten zu G-10 Maßnahmen wäre es zumindest sachdienlich gewesen, noch deutlicher auf das „Kerngeschäft" des BNDs hinzuweisen, nämlich die Auswertung des „offenen Himmels" nach Paragraph 1 Absatz 2 und Paragraph 2 Absatz I des BND-Gesetzes. Diese wichtige Praxis wird auch in den zweijährlichen allgemeineren Kontrollberichten des Gremiums nicht erwähnt. Zudem wäre es interessant gewesen, mehr darüber zu erfahren, inwiefern die Kontrolleure versucht haben, sich danach zu erkundigen, mit welchen Maßnahmen einer Vermischung der erfassten Telekommunikationsverkehre entgegengewirkt wird bzw. werden könnte. Wie eingangs bereits erwähnt, besteht gerade im Zuge der digitalisierten Kommunikation im Internet die Gefahr, dass auch innerdeutsche Kommunikationsverkehre in den Erfassungsgeräten des BNDs auftauchen könnten, wenn sie über ausländische Knotenpunkte geroutet werden.

Aufgrund der fast automatisierten und passiven Berichtspraxis des parlamentarischen Kontrollgremiums in Bezug auf die Beschränkungsmaßnahmen des G-10 Gesetzes und den fehlenden Angaben zur Erfassung des „offenen Himmels" in seinen Jahresberichten klingt die Vermutung eines ehemaligen Mitgliedes plausibel, dass einige Mitglieder des Gremiums von den strategischen Beschränkungsmaßnahmen nichts wüssten oder sie zumindest nicht mit dem Kontrollgremium in Verbindung setzen würden.

4.2 Wissensdefizite und Willensmängel

Bisher hat sich die kritische Bewertung der Kontrolltätigkeit vornehmlich auf das bezogen, was das Kontrollgremium selbst zu Protokoll gegeben hat. Die Diskrepanz zwischen dem, was das Kontrollgremium berichtet und dem, was der Bundesnachrichtendienst im Rahmen der strategischen Fernmeldeaufklärung unternimmt, wird aber noch deutlicher, wenn man sich die Antwort der Bundesregierung auf eine kleine Anfrage der Fraktion „Die Linke" vergegenwärtigt.[34]

Der BND darf gemäß Paragraph 10 des G-10 Gesetzes auf maximal zwanzig Prozent der Übertragungskapazität einer internationalen Leitung, die gebündelte Kommunikationsverkehre transportiert, zugreifen. Auf die Frage, wie viele Telekommunikationsverkehre im Zeitraum von 2002 bis 2012 täglich in die Erfassungssysteme des BNDs gelangten, und wie viele davon der Abschöpfung des „offenen Himmels" geschuldet waren, wich die Bundesregierung aus: „Eine statistische Erfassung im Sinne der Frage findet nicht statt. Sie ist gesetzlich nicht vorgesehen".[35]

Diese Antwort ist erstaunlich. Der Regierung – und somit den Kontrolleuren – fehlt die Kenntnis über die Gesamtmenge der vom BND täglich erfassten Kommunikationsverbindungen. Das ist vor dem Hintergrund der gesetzlichen Beschränkung der Erfassung auf 20% der Übertragungskapazität bemerkenswert. Ohne eine statistische Erfassung der Gesamtmenge kann die Zwanzig-Prozent-Hürde „getrost als willkürliche und vor allem wirkungslose Zahl gelten. Denn niemand weiß und niemand kontrolliert, wie

34 Drucksache des Bundestages 18/733.
35 Drucksache des Bundestages 18/733, S. 4

viel der BND tatsächlich belauscht".[36] Angesichts der technologischen Entwicklungen ist davon auszugehen, dass die Gesamtmenge im Vergleich zu 1999 dramatisch angestiegen ist. Damals wurden im Rahmen einer Verfassungsbeschwerde konkrete Zahlen genannt: 15.000 Telekommunikationsverkehre gerieten in die Umwandlungsgeräte des BNDs. Ein jüngst durch Edward Snowden enthülltes internes Memo eines GCHQ-Mitarbeiters attestiert dem BND beim Abgreifen von Telekommunikationsdaten und –Inhalten aus Glasfaserkabeln „riesige Möglichkeiten", einen „guten Zugang zum Herz des Internets" und eine Erfassung von „40 bis 100 Gigabit pro Sekunde".[37]

In den letzten Jahren hat sich also nicht nur in den USA und Großbritannien das Erfassen von digitalen Kommunikationsdaten drastisch verstärkt. Liest man aber die Berichte des Kontrollgremiums, so wird auf diesen Trend und die damit verbundenen rechtlichen und politischen Risiken nicht eingegangen. Wie zum Beispiel gewährleistet der BND bei der Verarbeitung der enormen Datenmengen, dass nicht doch Daten über deutsche Staatsbürger erfasst und weitergereicht werden? Diese Frage wäre ein wichtiger und überfälliger Gegenstand des nächsten Berichts des Kontrollgremiums.

Ein weiteres Wissensdefizit besteht im technischen Verständnis der strategischen Beschränkungsmaßnahmen und der Erfassung des „offenen Himmels". Ehemaligen Nachrichtendienstlern zufolge bestehen die Berichterstattungen des BNDs an die Bundesregierung mittlerweile zu mehr als fünfzig Prozent aus Informationen aus der strategischen Fernmeldeaufklärung. Um dieses zunehmend wichtige Geschäft besser zu verstehen, reicht es bei weitem nicht aus, sich ein Mal pro Jahr beim BND zu Besuch anzumelden. Was haben die Ingenieure des Bundesnachrichtendienstes für Erfassungsprogramme entwickelt, wie werden Kausalzusammenhänge erstellt und wer wacht dabei mit welchen Mitteln wie erfolgreich über die Einhaltung der gesetzlichen Vorschriften? Eine Stärkung der technischen Kompetenz scheint dringend nötig, wenn man bedenkt, dass die Mitglieder der G-10 Kommission den Großteil ihrer eigenen beruflichen Erfahrungen gemacht haben, bevor das Internet in der Massenkommunikation eine große Rolle spielte.[38]

Zum fehlenden Wissen über das Ausmaß der Internetüberwachung gesellt sich häufig ein fehlender Kontrollwille. Wenn die Bundesregierung ihrer Pflicht, das parlamentarische Kontrollgremium umfassend über die allgemeine Tätigkeit des Bundesnachrichtendienstes zu informieren, häufig nicht nachkommt, dann ist dies vielleicht auch dem Umstand geschuldet, dass die Mitglieder der einzelnen Kontrollgremien (parlamentarisches Kontrollgremium, G-10 Kommission und das Vertrauensgremium) höchst selten zusammenkommen. Wer sich untereinander kaum austauscht, lernt auch nicht aus dem jeweiligen Erfahrungsschatz der anderen Mitstreiter. Laut Angaben eines Mitglieds der G-10 Kommission wird dieser Austausch derzeit nicht gesucht. Gleichzeitig berichtet das parlamentarische Kontrollgremium stolz, dass sich Parlamentarier aus anderen Staaten „aufgrund des guten Rufs der hiesigen Kontrolle" regelmäßig an das Kontrollgremium mit dem Wunsch nach einem Erfahrungsaustausch wenden.[39] Aufgrund der deutlichen, mitunter selbstverschuldeten Kontrolldefizite stünde den deutschen Geheimdienstkontrolleuren mehr Reflektion über die Effektivität der eigenen Kontrolltätigkeit besser zu Gesicht.

4.3 Strukturelle Defizite

Ein wesentliches strukturelles Defizit bleibt die dürftige personelle Ausstattung der Kon-

36 Kai Biermann. 2014. Der BND ist nicht kontrollierbar. Zeit Online vom 14. März 2014.

37 Rosenbach, Marcel und Stark, Holger (2014): Der NSA Komplex. (München: DVA Verlag), S. 128.

38 Die Mitglieder der G-10 Kommission waren zum Ende des ersten goldenen Jahrzehnts der Internetüberwachung durchschnittlich 74 Jahre alt. Diese Zahlen gelten für das Jahr 2013. Im Januar 2014 ist das Durchschnittsalter der G-10 Kommission auf 64 Jahre gesunken.

39 Drucksache des Bundestages 18/217, S. 13.

trollgremien. Wie sollen ein knappes Dutzend vielbeschäftigter Parlamentarier und die vier unabhängigen Mitglieder der G-10 Kommission die Nachrichtendienste des Bundes mit ca. 10.500 Mitarbeitern umfassend kontrollieren können? Die Kontrolleure des parlamentarischen Kontrollgremiums können zwar zur Wahrnehmung ihrer Kontrolltätigkeiten auf Beschäftigte der Bundestagsverwaltung zurückgreifen, Mitarbeiter ihrer Fraktion ins Vertrauen ziehen und einen Sachverständigen einsetzen. Aber das reicht bei weitem nicht aus. In den letzten Jahren wurde auch in Deutschland verstärkt in die Nachrichtendienste investiert. Es wird Zeit, der Kontrolle ebenfalls einen angemessenen finanziellen und personellen Rahmen zu geben. Das erfordert jedoch einen gemeinsamen politischen Willen. Die erforderlichen Haushaltsmittel könnte der Bundestag schließlich jederzeit selbst bereitstellen.

Die parlamentarische Nachrichtendienstkontrolle legitimiert das Regierungshandeln. Je weniger die Möglichkeit besteht, die Kontrolle wirksam durchzuführen, desto weniger legitim ist das staatliche Handeln in diesem Politikfeld. In den geheimen Sitzungen des parlamentarischen Kontrollgremiums bestimmen die Kontrollierten weiterhin, dass die Kontrolleure keine Notizen machen dürfen. Was immer in den Sitzungen besprochen wird, wird den Kontrolleuren als „Tischvorlage“ gereicht. Scheidet ein Kontrollgremiumsmitglied aus, kann mitunter das gesamte Kontrollgedächtnis einer Fraktion erlöschen.

Das parlamentarische Kontrollgremiums-Gesetz (und wie eingangs berichtet auch das G-10 Gesetz) ist an vielen Stellen zu vage. Was sind eigentlich die nachrichtendienstlichen Mittel des BNDs?[40] Welche Idealtypen gibt es für „Vorgänge von besonderer Bedeutung“, über die die Bundesregierung zu berichten hat? Welche Konsequenzen ergeben sich, wenn die Bundesregierung ihrer Unterrichtungspflicht zu spät oder gar nicht nachkommt?

Je weiter die Kontrolleure in den Kernbereich der Regierungsführung vordringen, desto wahrscheinlicher sind Streitigkeiten über den Zugang zu vertraulichen Informationen. Hier fehlt vor allem eine institutionalisierte Rechtskontrolle über die Geheimhaltungseinstufung - eine Streitschlichtungsstelle, die idealerweise zeitnah und unbürokratisch eine Lösung herbeiführt. Zuletzt musste die qualifizierte Minderheit im BND-Untersuchungsausschuss ein Organstreitverfahren beim Bundesverfassungsgericht anstrengen, um mit über zwei Jahren Verspätung und nach Abschluss der Untersuchungen eine klärende Antwort zu erhalten.

4.4 Ergebniskontrolle, informationstechnische Dienstvorschriften und internationale Kooperation

Nach eigenen Angaben widmen sich die Mitglieder der G-10 Kommission vollständig den Zulässigkeitsentscheidungen und den Mitteilungspflichten. Mitarbeiter der Bundestagsverwaltung arbeiten sowohl dem parlamentarische Kontrollgremium als auch der G-10 Kommission zu. Für die G-10 Kommission koordinieren sie beispielsweise die monatlichen Sitzungen und sichten bereits im Vorfeld die übermittelten Anordnungen von Beschränkungsmaßnahmen. Der G-10 Kommission fehlen aber die Kapazitäten für eine Ergebniskontrolle der Maßnahmen. Weder das parlamentarische Kontrollgremium noch das Vertrauensgremium haben in den letzten Jahren über Untersuchungen berichtet, in denen sie den Aufwand der Beschränkungsmaßnahmen mit deren Ergebnissen in Beziehung gesetzt haben.[41]

40 Interessanterweise finden sich auf Länderebene bedeutend bestimmtere Gesetze. In §8 BremVerfSchG werden beispielsweise die nachrichtendienstlichen Mittel einzeln aufgezählt.

41 Das Vertrauensgremium ist ein Instrument der Finanzkontrolle über die Nachrichtendienste des Bundes. Der Bundestag wählt die Mitglieder des Vertrauensgremiums aus dem Kreis des Haushaltsausschusses. Das Bundesfinanzministerium hat die Wirtschaftspläne für die Nachrichtendienste des Bundes dem Vertrauensgremium zur Billigung vorzulegen. Es berichtet dem Bundestag zweimal pro Wahlperiode über seine Kontrolltätigkeit. Der letzte Bericht ist in Drucksache des Bundestages 17/14344 aufgeführt.

Aus Nachrichtendienstkreisen wurde auch über eine „Dienstvorschrift informationstechnische Operationen“ (DITO) berichtet, die vermutlich der dritten Methode der technischen Aufklärung, „spezielle Operationen“, zuzuordnen ist. Sie soll dem BND weitere Kompetenzen unter anderem im Bereich des Hackings zuweisen. Weder das Erlassen noch die Umsetzung dieser Dienstvorschriften unterliegen der parlamentarischen Kontrolle. Das parlamentarische Kontrollgremium wird lediglich vom zuständigen Bundesministerium informiert.

Die Enthüllungen von Edward Snowden zeigen, dass westliche Geheimdienste die Informationen aus der Überwachung digitaler Telekommunikationsverkehre miteinander teilen beziehungsweise sie ihren ausländischen Partnern im Rahmen eines Tauschgeschäftes anbieten. Der vom Bundestag im April 2014 eingesetzte NSA-Untersuchungsausschuss will nun in Erfahrung bringen, inwiefern „Stellen des Bundes (…) Teil eines systematisierten wechselseitigen ‚Ring-Tausches‘ geheimdienstlicher Informationen (waren), in dem der jeweils anderen Seite Daten oder Erkenntnisse übermittelt werden, die diese nach dem jeweils am Ort der Datenerhebung geltenden Rechts selbst nicht erheben (dürfen)“.[42] Das parlamentarische Kontrollgremium berichtet turnusgemäß über die Übermittlungen von Informationen an „bestimmte ausländische öffentliche Stellen“, bezieht sich jedoch nur auf eine bestimmte Beschränkungsmaßnahme des G-10 Gesetzes und wusste im Zeitraum von Januar 2010 bis Dezember 2013 lediglich von drei solcher Übermittlungen zu berichten.[43] Bei der Auswertung des „offenen Himmels“ ist die Bundesregierung auf internationale Kooperation angewiesen und hat daher mit über 40 internationalen Partnern ein Memorandum of Understanding abgeschlossen. Darin werden die Modalitäten der Abschöpfung von Informationen aus Seekabeln in fremden Ländern bilateral festgehalten. Dass Nachrichtendienste Informationen miteinander tauschen, sollte niemanden verwundern. Heikel wird es allerdings dann, wenn der Informationsaustausch rechtstaatliche Hürden und die parlamentarische Kontrolle aushebelt. Ob dies der Fall ist, kann derzeit nicht geprüft werden. Ausländische Partnerdienste teilen Ihre Informationen häufig nur unter der Bedingung, dass der Empfänger die Daten nicht ohne Zustimmung des Senders mit Dritten teilt. In der Praxis gelten nationale Kontrollgremien ebenfalls als „Dritte“.

4.5 Empfehlungen für eine verbesserte parlamentarische Kontrolle

Die strategische Fernmeldeaufklärung des BNDs wird kaum kontrolliert. Das Parlamentarische Kontrollgremium ist in seiner jetzigen Aufstellung nicht in der Lage, dem seit 2009 auch im Grundgesetz verbrieften Kontrollauftrag gerecht zu werden. Es besteht ein eklatantes Missverhältnis zwischen dem Kompetenz- und Bedeutungszuwachs der Nachrichtendienste einerseits, und den eher kleinen gesetzlichen Novellierungen, der groben Unterfinanzierung und der Antriebsarmut der parlamentarischen Kontrolle andererseits.

Die beeindruckende Bandbreite der im vorherigen Abschnitt erörterten Kontrolldefizite und Wissenslücken ist in der nachfolgenden Tabelle zusammengefasst.

42 Drucksache des Bundestages 18/843 unter B.I.7.

43 Seit Januar 2010 wurde insgesamt nur über drei Übermittlungen von Informationen an ausländische Partner aus Beschränkungsmaßnahmen nach §5 Absatz 1 Satz 3 Nummer 2,3 und 7 G-10-Gesetz berichtet. Siehe Drucksachen des Bundestages 18/218, 17/12773, und 17/8639.

Tabelle 2: Entscheidende Defizite der gegenwärtigen parlamentarischen ND-Kontrolle

Kontrollfreie Bereiche (Internationale ND-Kooperation; Erlassen und Umsetzen geheimer Dienstvorschriften)	Eingeschränkte Möglichkeit, Geheimhaltungsentscheidungen und den Zugang zu Informationen zeitnah richterlich zu prüfen	Unpräzise und zu spät veröffentlichte Kontrollberichte
Unspezifische Rechtsnormen (was genau sind „Vorgänge von besonderer Bedeutung“?)	Kaum Sanktionsmöglichkeiten gegenüber der Bundesregierung oder den Diensten bei offensichtlichem Fehlverhalten (z.B. stone-walling; slow-rolling)	Ungenügend Zeit und Ressourcen für den Kontrollauftrag
Ungenügend Informationen über die strategische Fernmeldeaufklärung und deren parlamentarische Kontrolle	Kaum strukturierter Austausch zwischen den Mitgliedern der verschiedenen Kontrollgremien	Fehlende kritische Distanz zum Berichtsgegenstand
Unzureichende Kontrollbefugnis (z.B. Tischvorlage ohne Möglichkeit, Notizen zu nehmen)	Fehlendes Detailwissen über die Gesamterfassung von Kommunikationsdaten des BND	Begrenztes IT-Verständnis

Die defizitäre Situation der parlamentarischen Nachrichtendienstkontrolle schlägt umso gravierender zu Buche, da in Deutschland keine institutionalisierte richterliche Kontrolle über die Überwachung der Telekommunikationsverkehre durch die Nachrichtendienste des Bundes existiert.

„Wir wollen eine bessere parlamentarische Kontrolle der Nachrichtendienste“, bekunden Union und SPD in ihrem Koalitionsvertrag. Dieses Bekenntnis haben interessierte Beobachter der Innen- und Sicherheitspolitik in den letzten Jahren häufig gehört. Mittlerweile haben einige Politiker erkannt, dass eine funktionierende Nachrichtendienstkontrolle nicht nur demokratietheoretisch wichtig ist. Sie hat auch eine enorme strategische Bedeutung. Ein weitgehend unkontrollierter Nachrichtendienstbereich, wie die strategische Fernmeldeaufklärung, kann erheblichen politischen Flurschaden anrichten, wie man es zurzeit an den Enthüllungen über die NSA sehr gut beobachten kann.

Will das Parlament seinen verfassungsmäßigen Kontrollauftrag tatsächlich erfüllen, so sind wesentliche Maßnahmen umzusetzen, um die Ziele – mehr Kontrolleffizienz, weniger Politisierung und mehr Transparenz – zu verwirklichen. Die Umsetzung folgender Handlungsempfehlungen halten wir für zielführend:

Erstens benötigen wir dringend die Entwicklung eines umfassenden Kriterienkatalogs für die parlamentarische Nachrichtendienstkontrolle. Nur das, was man messen kann, kann man auch nachhaltig reformieren. Noch haben wir ein viel zu oberflächliches Verständnis von der Kontrolltätigkeit. Natürlich setzt der Geheimschutz den Kontrolleuren Grenzen in Bezug auf das, was sie der Öffentlichkeit berichten können. Noch sind diese aber bei weitem nicht ausgeschöpft und mehr Transparenz wäre nicht nur vertretbar, sondern sogar notwendig. Die Berichte der Kontrollgremien sind im internationalen Vergleich knapp und vage formuliert. Erkenntnisse der neueren Verwaltungswis-

senschaft zeigen, wie man beispielsweise die Berichts- und Unterrichtungspflichten der Exekutive und das Kontrollverhalten der Kontrolleure besser spezifizieren und indexieren könnte.[44]

Im Kontrollgremium ließe sich beispielsweise darüber abstimmen, inwieweit nach Meinung der Kontrolleure die Bundesregierung ausreichend ihrer Unterrichtungspflicht pro Themenfeld nachgekommen ist. Das Stimmverhalten könnte man dann in den öffentlichen Berichten an den Bundestag protokollieren. Auch ließe sich dokumentieren, inwieweit die Mitglieder des parlamentarischen Kontrollgremiums ihr Recht wahrgenommen haben, an den Sitzungen des Vertrauensgremiums teilzunehmen. Damit ließe sich der Druck auf die zurückhaltenderen Mitglieder in den Kontrollgremien erhöhen. Gerade weil die Nachrichtendienste so an Bedeutung gewonnen haben und weil die richterliche Kontrolle in Deutschland so schwach ist, sollten die Kontrolleure angehalten werden, nicht nur ihr Output (z.B. das Veröffentlichen eines Abschlussberichts; das Abhalten von Sitzungen und Zeugenvernehmungen) in den Vordergrund der Unterrichtungen zu stellen, sondern ihre Kontrolltätigkeit auch gemäß dynamischen Indikatoren und internationalen Qualitätsstandards zu protokollieren.[45] Mit Hilfe eines Kriterienkatalogs ließen sich aufwendige aber wenig effektive Aufklärungszeremonien als solche identifizieren. Dies wäre ein wichtiger Schritt, um den Weg für die Verwendung von wirkungsvolleren Kontrollinstrumenten zu ebnen.

Zweitens benötigen wir die systematische Förderung des Austausches zwischen den einzelnen Kontrollgremien des Bundestages. Besonders wichtig ist hierbei ein regelmäßiger Austausch zwischen den Mitgliedern der G-10 Kommission, dem parlamentarischen Kontrollgremium und dem Vertrauensgremium unter Einbeziehung des Bundesbeauftragten für den Datenschutz und die Informationssicherheit. Welche Erfahrungen haben die einzelnen Kontrollgremien mit welchen Kontrollmitteln gemacht (zum Beispiel über Ermittlungen durch externe Sachverständige; öffentliche Stellungnahmen; Sach- und Personalausstattung) und wie ließe sich der gemeinsame Erfahrungsschatz in Zukunft besser nutzen? Hierbei wäre es auch hilfreich, den Austausch mit externen Wissenschaftlern und Nichtregierungsorganisationen in einer gewissen Regelmäßigkeit zu institutionalisieren.

Drittens ist es begrüßenswert, wenn der Vorsitzende des parlamentarischen Kontrollgremiums vor kurzem weiterführende Reformvorschläge wie die Einführung eines operativen Stabs aus fünf bis acht zusätzlichen Mitarbeitern zur Unterstützung der

44 Siehe Brandsma, Gijs J. und Schillemans, Thomas (2012): The accountability cube: Measuring Accountability. Journal of Public Administration Research and Theory. Heft 23, Nummer 4, S. 953-975. Bovens, Mark (2007): Analysing and Assessing Accountability: A conceptual framework. European Law Journal. Heft 13, Nummer 4, 447-468; Wetzling, Thorsten (2010):Same myth, different celebration? Intelligence accountability in Germany and the United Kingdom. (Genf: Graduate Institute for International and Development Studies).

45 Nennenswert sind hier die folgenden Beschlüsse bzw. Studien: UN Human Rights Council (2010): Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight. A/HRC/14/46; European Commission for Democracy through Law (Venice Commission) (2007): Report on the democratic oversight of the security services. CDL-AD; Born, Hans und Leigh, Ian (2005): Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies (Oslo: Publishing House of the Norwegian Parliament). Unlängst hat das United Nations Human Rights Committee wesentliche Forderungen aufgegriffen, siehe United Nations(2014):Concluding observations on the fourth periodic report of the United States of America. CCPR/C/USA/CO/4, Punkt 22.

Ermittlungstätigkeit anvisiert.[46] Dennoch ist der mitunter sehr kontraproduktiven Politisierungsdynamik zwischen Regierungsmehrheit und Oppositionsvertretern in den Kontrollgremien wohl besser mit der Schaffung eines unabhängigen und mit ausreichend personellen Ressourcen ausgestatteten Nachrichtendienstbeauftragten entgegenzutreten.

Viertens sind die Kosten für das Nichtzusammenarbeiten mit dem parlamentarischen Kontrollgremium durch Einführung eines Dienstvergehens bei unterlassener Unterrichtung durch die Bundesregierung zu erhöhen. Bisher hat das parlamentarische Kontrollgremium keine effektiven Mittel zur Hand, um gegen etwaiges stone-walling (Abwehr von Auskunftsgesuchen) oder slow-rolling (Verzögerung in der Bearbeitung von Auskunftsgesuchen) der Bundesregierung wirksam vorzugehen. Hierzu gehört auch die fehlende Möglichkeit, die von der Bundesregierung festgelegten Geheimhaltungsbestimmungen noch während einer laufenden Untersuchung einer richterlichen Kontrolle zuzuführen. Der einzig gangbare Weg des Organstreitverfahrens beim Bundesverfassungsgericht hat sich in der Vergangenheit als zu langwierig und zu komplex erwiesen.

Schließlich ist gerade im Hinblick auf das Kerngeschäft des BNDs – die strategische Fernmeldeaufklärung – das IT-Verständnis der Kontrolleure durch umfassende und regelmäßige Schulungen zu erhöhen. Zusätzlich schlagen wir die Einrichtung eines versierten IT-Stabs mit ausreichender Sicherheitsüberprüfung vor.

Schlussbemerkungen

Die Vereinigten Staaten haben damit begonnen, sich mit den rechtlichen Grundlagen und der Kontrolle der NSA auseinanderzusetzen. Expertenkommissionen haben getagt und bereits Berichte vorgelegt und mehrere Reformgesetze sind in den Kongress eingebracht worden. Aus deutscher Sicht gehen die amerikanischen Reformanstrengungen sicher nicht weit genug. Insbesondere die unterschiedliche Behandlung von US-Personen und Ausländern bleibt ein großes Problem. Unsere berechtigte Kritik an amerikanischen Überwachungsprogrammen können wir aber nur glaubhaft vortragen, wenn wir uns auch mit unseren eigenen Diensten und ihren Praktiken kritisch auseinandersetzen. Auch das Ziel, eine internationale Debatte über Überwachungsstandards zumindest unter demokratischen Rechtsstaaten anzustoßen, kann nur erreicht werden, wenn wir uns mit den rechtlichen Grundlagen und der Kontrolle unserer eigenen nachrichtendienstlichen Auslandsaufklärung befassen. Rechtliche Grundlagen und Kontrolle sollten hierbei in einem Gesamtbild betrachtet werden. Denn wie wir hier gezeigt haben, wird es nicht ausreichen, das G-10 Gesetz einfach auch auf die strategische Auslandsaufklärung anzuwenden. Wir brauchen zusätzlich klare Normen für die Befugnisse der Nachrichtendienste, genauso wie effektive Kontrollinstitutionen, die die Einhaltung dieser Normen gewährleisten.

Um dies zu erreichen, ist vor allem der Bundestag gefordert. Der Bundestag steht hier in der Verantwortung gegenüber den Bürgerinnen und Bürgern – zum einen in seiner Rolle als Kontrolleur der Nachrichtendienste – und zum anderen in seiner Rolle als Gesetzgeber, der sowohl den Auftrag wie auch die Grenzen nachrichtendienstlicher Praktiken und den Kontrollrahmen zu definieren hat.

46 http://www.tagesspiegel.de/politik/parlamentarisches-kontrollgremium-reform-in-homoeopathischen-dosen/9613950.html

Ausgewähltes Literaturverzeichnis

Bäcker, Matthias (2014): Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stellungnahme zur Anhörung des NSA Untersuchungsausschusses am 22. Mai, 2014

Biermann, Kai (2014): Der BND ist nicht kontrollierbar. Zeit Online vom 14. März.

Born, Hans und Leigh, Ian (2005): Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies (Oslo: Publishing House of the Norwegian Par-liament).

Bovens, Mark (2007): Analysing and Assessing Accountability: A conceptual framework. European Law Journal. Heft 13, Nummer 4, 447-468.

Brandsma, Gijs J. und Schillemans, Thomas (2012): The accountability cube: Measuring Account-ability. Journal of Public Administration Research and Theory. Heft 23, Nummer 4, S. 953-975.

Caspar, Johannes (2014): Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats? Privacy in Germany, Heft 1/2014, S. 1-6.

European Commission for Democracy through Law (Venice Commission) (2007): Report on the democratic oversight of the security services. CDL-AD.

European Parliament LIBE Committee Inquiry (2014): Electronic Mass Surveillance of EU Citizens: Protecting fundamental rights in a digital age – Proceedings, Outcomes and Background Documents

Heumann, Stefan und Scott, Ben (2013): Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany. (Berlin: stiftung neue verantwortung).

Hörauf, Dominic (2011): Die demokratische Kontrolle des Bundesnachrichtendienstes: Ein Rechtsvergleich vor und nach 9/11. (Hamburg: Verlag Dr. Kovać).

Huber, Bertold (2013): Die strategische Rasterfahndung des Bundesnachrichtendienstes – Ein-griffsbefugnisse und Regelungsdefizite. Neue Juristische Wochenschrift, Heft 35/2013, S.2572-2577.

Rosenbach, Marcel und Stark, Holger (2014): Der NSA Komplex. (München: DVA Verlag).

United Nations Human Rights Committee (2014):Concluding observations on the fourth periodic report of the United States of America. CCPR/C/USA/CO/4

United Nations Human Rights Council (2010): Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Com-pilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight. A/HRC/14/46.

Wetzling, Thorsten (2014): Das Geheimnis der Geheimdienstkontrolle, Blätter für deutsche und internationale Politik. Heft 2/2014., S. 57-62.

Wetzling, Thorsten (2010). Same myth, different celebration? Intelligence accountability in Ger-many and the United Kingdom. (Genf: Graduate Institute for International and Development Studies).

Drucksachen des Bundestages

Drucksache 17/8639. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht gemäß §14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses über die Durchführungen sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes. (Berichtzeitraum 1. Januar bis 31. Dezember 2010), 10.02.2012

Drucksache 17/12773. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht gemäß §14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses über die Durchführungen sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes. (Berichtzeitraum 1. Januar bis 31. Dezember 2011), 14.03.2013.

Drucksache 17/14344. Unterrichtung durch das Vertrauensgremium gemäß §10a Absatz 2 der Bundeshaushaltsordnung. Bericht über die Tätigkeit des Vertrauensgremiums im Zeitraum Januar 2012 bis Juni 2013, 05.07.2013.

Drucksache 18/217. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht über die Kontrolltätigkeit gemäß §13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes. (Berichtzeitraum November 2011 bis Oktober 2013, 09. Dezember 2013.

Drucksache 18/218. Unterrichtung durch das Parlamentarische Kontrollgremium. Bericht gemäß §14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses über die Durchführungen sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses Gesetzes. (Berichtzeitraum 1. Januar bis 31. Dezember 2012), 19.12.2013.

Drucksache 18/733. Antwort der Bundesregierung auf die Kleine Anfrage (Drucksache 18/553) zur strategischen Rasterfahndung des Bundesnachrichtendienstes im Zeitraum 2002 bis 2012, 05.03.2014

Drucksache 18/843. Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE und BÜNDNIS 90/DIE GRÜNEN zur Einsetzung eines Untersuchungsausschusses, 18.03.2014.

Dr. Thorsten Wetzling ist Senior Research Fellow am Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS) in Potsdam. Zuvor war er als Senior Fellow am Institute for Global Justice in Den Haag und als Berater für das Geneva Centre for the Democratic Control of Armed Forces (DCAF) tätig. Dort leitete er Projekte zum Datenschutz in den transatlantischen Beziehungen so-wie zur Reform des Sicherheitssektors in Marokko und Tunesien. Thorsten Wetzling hat am Genfer Hochschulinstitut für Internationale Studien und Entwicklung mit einer vergleichenden Studie zur Performanz und Reform der Nachrichtendienstkontrolle in Europa promoviert.

Dr. Stefan Heumann ist stellvertretender Leiter des Programms „Europäische Digitale Agenda“ bei der stiftung neue verantwortung. Das Programm bringt zentrale Akteure und Vordenker aus Wirtschaft, Gesellschaft und Politik zusammen, um sich strategisch mit den politischen Herausforderungen von Digitalisierung zu befassen und gemeinsam Handlungsoptionen zu diskutieren und zu entwickeln. Im Rahmen des Privacy Project befasst sich das Programm mit Fragen des Grundrechtsschutzes in Zeiten von Big Data und staatlicher Überwachung. Dr. Heumann hat Politikwissenschaft an der FU Berlin studiert und an der University of Pennsylvania promoviert. Nach Stationen als Assistant Professor an der University of Northern Colorado und Koordinator der Öffentlichkeits- und Programmarbeit des US-Generalkonsulats in Hamburg kam er im Mai 2013 zur stiftung neuen verantwortung.

Die stiftung neue verantwortung ist ein unabhängiger, gemeinnütziger und überparteilicher Think Tank mit Sitz in Berlin. Sie fördert kreatives, interdisziplinäres und sektorübergreifendes Denken zu den wichtigsten gesellschaftspolitischen Themen und Herausforderungen des 21. Jahrhunderts. Durch ihr Fellow- und Associateprogramm ermöglicht sie den intensiven Austausch junger Experten, Praktiker und Vordenker aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes Institut in Potsdam mit der Mission, Brücken zwischen Theorie und Praxis zu bauen, um die zivile Sicherheit durch einen multi- und interdisziplinären Ansatz zu erhöhen. Indem nationale wie internationale Multiplikatoren aus Politik, Wirtschaft, Verwaltung, Medien und Wissenschaft zusammengeführt werden, schafft das BIGS innovative Strategien und Lösungen für die Bedrohungen, mit denen freiheitlich-demokratische Staaten in der Gegenwart und in der Zukunft konfrontiert werden. Einen besonderen Forschungsschwerpunkt hat das BIGS in ökonomischen Fragen von Sicherheit sowie in der Analyse der Sicherheitswirtschaft.

Impressum

Gestaltung:
Pentagram Design, Berlin

Schlusslektorat:
Franziska Wiese, Wera Patten

Kostenloser Download:
www.stiftung-nv.de

stiftung neue verantwortung e.V.
Stefan Heumann
Stellv. Programmleiter „Europäische Digitale Agenda“
Beisheim Center
Berliner Freiheit 2
10785 Berlin
T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97
www.stiftung-nv.de
sheumann@stiftung-nv.de