Deutscher Bundestag **Drucksache 17/14714**

17. Wahlperiode 06. 09. 2013

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/14515 –

Neuere Formen der Überwachung der Telekommunikation durch Polizei und Geheimdienste

Vorbemerkung der Fragesteller

Berichte über die zunehmende Überwachung und Analyse digitaler Verkehre untergraben das Vertrauen in die Freiheit des Internets und der Telekommunikation. Aus den Antworten aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz „stiller SMS“, so genannter WLAN-Catcher und IMSI-Catcher nimmt stetig zu, die Ausgaben für Analysesoftware steigen ebenfalls. Auch die Fähigkeiten zur Bildersuche in Polizeidatenbanken werden weiterentwickelt, beispielsweise nutzt das Bundeskriminalamt immer häufiger die Möglichkeit der Abfrage seiner Datenbestände mittels Aufnahmen aus Überwachungskameras. Neuere Meldungen über Fähigkeiten in- und ausländischer Geheimdienste sind weiterer Anlass zu großer Besorgnis: Britische, US-amerikanische, aber auch deutsche Behörden filtern den Telekommunikationsverkehr und durchsuchen diesen nach Schlüsselbegriffen. Der Bundesminister des Innern, Dr. Hans-Peter Friedrich, rechtfertigt diese Praxis damit, dass es ein „Supergrundrecht“ auf Sicherheit gebe (DIE WELT, 16. Juli 2013). Die Fragesteller sind demgegenüber der Ansicht, dass Grundrechte nicht hierarchisiert werden können. Die Aussage des Bundesministers ist eine nicht zu rechtfertigende Diskreditierung der Freiheit.

Um das gestörte Vertrauen in das Fernmeldegeheimnis wieder herzustellen fordern die Fragesteller die regelmäßige Veröffentlichung aller Stichworte, die von Behörden wie dem Bundesnachrichtendienst zur Durchsuchung digitaler Kommunikation genutzt werden.

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 2, 5, 9, 10, 13, 17, 18, 19, 22, 25, 26, 33, 34 sowie 36 in offener Form ganz oder teilweise nicht erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der Sicher-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 4. September 2013 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

heitsbehörden und insbesondere seinen Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des Bundesnachrichtendienstes im Rahmen der Fernmeldeaufklärung stellt für die Aufgabenerfüllung des Bundesnachrichtendienstes einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde zu einer wesentlichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung des Bundesnachrichtendienstes erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen und damit das Staatswohl gefährden. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Geheim“ eingestuft und werden über die Geheimschutzstelle des Deutschen Bundestags zugeleitet.

Die Antwort auf die Kleine Anfrage beinhaltet zum Teil detaillierte Einzelheiten zu den technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen der Behörden der Zollverwaltung. Aus ihrem Bekanntwerden könnten Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Ermittlungsbehörden gezogen werden. Deshalb sind die entsprechenden Informationen gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) als „VS-Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Dies betrifft im Einzelnen die Antworten zu der Frage 4.

1. Nach welchen, mehreren Tausend Suchbegriffen durchforstet der Bundesnachrichtendienst die digitale Telekommunikation im Rahmen seiner „Strategischen Fernmeldeaufklärung“ (Bundestagsdrucksache 17/9640)?

Die für die Durchführung von strategischen Beschränkungsmaßnahmen nach §§ 5 und 8 des Gesetzes über die Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-Gesetz) beantragten Suchbegriffe werden durch die zuständigen auswertenden Abteilungen des Bundesnachrichtendienstes (BND) anhand am Aufklärungsprofil orientierter, fachlicher und technischer Erwägungen unter Berücksichtigung der gesetzlichen Vorgaben festgestellt. Die Anordnung erfolgt durch das Bundesministerium des Innern nach Maßgabe der §§ 9, 10 G10 mit Zustimmung der G10-Kommission, § 15 Absatz 5, 6 G10.

Nach sorgfältiger Abwägung zwischen dem aus Artikel 38 Absatz 1 Satz 2 i. V. m. Artikel 20 Absatz 2 Satz 2 des Grundgesetzes (GG) resultierenden Informationsrecht des Deutschen Bundestages einerseits und den hier vorliegenden Geheimhaltungsinteressen andererseits ist die Bundesregierung zu der Auffassung gelangt, dass im Rahmen einer Kleinen Anfrage die Nennung von Suchbegriffen im Sinne der Anfrage aus Gründen des Staatswohls nicht erfolgen kann. Hierbei waren folgende Erwägungen leitend:

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Die Verwendung von Suchbegriffen durch den BND dient der Aufklärung von Sachverhalten in nachrichtendienstlich relevanten Gefahrbereichen. Die Suchbegriffe spiegeln unmittelbar Arbeitsweisen, Strategien, Methoden und Erkenntnisstand des BND in allen Bereichen der dem BND zugewiesenen Aufgabenbereiche wider. Ihre Offenlegung würde daher dessen Arbeitsfähigkeit und Aufgabenerfüllung in erheblichem Maße beeinträchtigen oder sogar vereiteln. Aus diesem Grund sind die erfragten Informationen von solcher Bedeutung, dass auch ein nur geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]), weshalb selbst eine Einstufung der Antwort als Verschlusssache und deren Übermittlung über die Geheimschutzstelle des Deutschen Bundestages nicht in Betracht kommt. Dem Informationsrecht des Deutschen Bundestages ist gleichwohl dadurch Rechnung getragen, dass die Verwendung der Suchbegriffe der Genehmigung der G10-Kommission des Deutschen Bundestages bedarf. Diese sehr weite Genehmigungszuständigkeit des Parlaments für exekutives Handeln gleicht die Einschränkungen beim Kreis der informationszugangsberechtigten Personen aus. Das der Bundesregierung verfassungsrechtlich auferlegte Gebot, den Deutschen Bundestag in die Lage zu versetzen, seine Aufgabe der parlamentarischen Kontrolle des Regierungshandeln effektiv wahrzunehmen (vgl. BVerfGE 124, 161 [192]), ist dadurch erfüllt. Der Gesetzgeber hat mit dem G10 eine Balance zwischen dem parlamentarischen Kontrollrecht und nachrichtendienstlichen Geheimhaltungsinteressen hergestellt, indem er der zur Gewährleistung der Geheimhaltung erforderlichen Beschränkung der Anzahl der informationszugangsberechtigten Personen weitgehende parlamentarische Kontroll- und Genehmigungsbefugnisse zur Seite gestellt hat. Die Bundesregierung ist der Auffassung, dass dadurch im Sinne praktischer Konkordanz sowohl den nachrichtendienstlichen Geheimhaltungsinteressen wie auch der parlamentarischen Kontrolle in einer Weise Rechnung getragen worden ist, die beide optimal zur Geltung kommen lässt.

2. Welche Bundesbehörden (außer Zoll) sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone so genannte stille SMS zum Ausforschen des Standortes ihrer Besitzer oder dem Erstellen von Bewegungsprofilen zu verschicken, und wie oft wurden die Maßnahmen im Vergleich zur Antwort auf die Schriftliche Frage 14 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 17/8102 im Jahr 2012 sowie dem ersten Halbjahr 2013 von den jeweiligen Behörden jeweils vorgenommen (bitte auch die jährliche Gesamtzahl der verschickten „Ortungsimpulse“ nennen)?

Die folgenden Bundesbehörden sind sowohl technisch als auch rechtlich in der Lage, sogenannte Stille SMS an Mobiltelefone zu versenden und haben dies im dargestellten Umfang getan:

Jahr	BfV	BND	BKA	BPOL	MAD
2012	28 843	(1)	37 352	63 354	1
2013 (bis 30.06.)	28 472	(1)	31 948	65 449	–

(1) Einstufung als Verschlusssache VS-Geheim.*

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

3. Sofern für den Militärischen Abschirmdienst (MAD) weiterhin keine Angaben gemacht werden, inwiefern wird die Technik von diesem überhaupt genutzt, in welcher Größenordnung liegt deren Anwendung und in welchen Bereichen wird diese eingesetzt?

Auf die Antwort zu Frage 2 wird verwiesen.

4. Welche Zollbehörden sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone so genannte stille SMS zum Ausforschen des Standortes ihrer Besitzer oder dem Erstellen von Bewegungsprofilen zu verschicken, und wie oft wurden die Maßnahmen im Vergleich zur Antwort auf die Schriftliche Frage 14 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 17/8102 im Jahr 2012 sowie dem ersten Halbjahr 2013 von den jeweiligen Behörden jeweils vorgenommen (bitte auch die jährliche Gesamtzahl der verschickten „Ortungsimpulse“ nennen und nach Zollkriminalamt und einzelnen Zollfahndungsämtern aufschlüsseln)?

Die zuständigen Behörden der Zollverwaltung sind auf Grundlage richterlichen Beschlusses im Rahmen ihrer Aufgabenerfüllung zur Versendung von Ortungsimpulsen (sogenannte Stille SMS) berechtigt. Im Jahr 2012 wurden 199 023 Ortungsimpulse versendet und im ersten Halbjahr 2013 138 779.

Die Gesamtanzahl der Ortungsimpulse entfällt auf das Zollkriminalamt (ZKA) und die acht Zollfahndungsämter Berlin-Brandenburg, Dresden, Essen, Frankfurt/Main, Hamburg, Hannover, München und Stuttgart. Ebenfalls hierin berücksichtigt sind Verfahren der Finanzkontrolle Schwarzarbeit der Zollverwaltung (FKS), soweit das Zollkriminalamt tätig geworden ist.

Soweit für die FKS Ortungsimpulse nicht durch das ZKA oder die Zollfahndungsämter (ZFA), sondern in Amtshilfe durch die Bundespolizei oder die Landespolizeien versandt wurden, liegen hierzu keine statistischen Daten der Zollverwaltung vor.

Es gilt zu berücksichtigen, dass aus den Zahlen keine Rückschlüsse auf den Umfang des tatsächlich betroffenen Personenkreises gezogen werden können, da die Anzahl der in einem einzelnen Verfahren wiederkehrend versendeten Ortungsimpulse von diversen Faktoren, wie bspw. Verfahrensumfang und -dauer, abhängt.

Hinsichtlich der Aufschlüsselung nach Zollkriminalamt und den einzelnen Zollfahndungsämtern wird auf den VS-NfD eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

5. Mit welchen Anwendungen (Hard- und Software) welcher Hersteller werden die „stillen SMS“ gegenwärtig versandt, und welche Änderungen haben sich hierzu in den letzten Jahren ergeben?

Auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.**

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden (diese Regelung gilt noch befristet bis zum Ende der 17. Legislaturperiode.

** Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

6. Welche Bundesbehörden haben seit 2007 wie oft „IMSI-Catcher“ eingesetzt (bitte nach einzelnen Jahren aufschlüsseln und auch für das erste Halbjahr 2013 angeben)?

Für den Bundesverfassungsschutz (BfV), BND und den Militärischen Abschirmdienst (MAD) wird hinsichtlich der Jahre 2007 bis 2011 auf die als Bundestagsdrucksache veröffentlichten jährlichen Unterrichtungen durch das Parlamentarische Kontrollgremium (§§ 8a Absatz 6 Satz 2, 9 Absatz 4 Satz 7 des Bundesverfassungsschutzgesetzes (BVerfSchG] a. F. bzw. §§ 8b Absatz 3 Satz 2, 9 Absatz 4 Satz 7 BVerfSchG n. F., ggf. i. V. m. § 3 Satz 2 des Bundesnachrichtendienstgesetzes – BNDG – oder § 5 des Gesetzes über den Militärischen Abschirmdienst – MADG) verwiesen.

In den Jahren 2012/2013 hat

- das BfV IMSI-Catcher in 16 Fällen in 2012 eingesetzt, im ersten Halbjahr 2013 erfolgten 18 Einsätze
- der BND IMSI-Catcher in einem Fall in 2012 eingesetzt, im ersten Halbjahr 2013 erfolgte kein Einsatz und
- der MAD IMSI-Catcher weder in 2012 noch in 2013 eingesetzt.

BKA, BPOL und Zoll haben IMSI-Catcher entsprechend nachstehender Tabelle eingesetzt. In den Gesamtzahlen können Amtshilfefälle für andere Landes- oder Bundesbehörden enthalten sein.

Zeitraum	BKA	BPOL	Zoll
2007	31	40	unbekannt
2008	33	42	21
2009	45	46	33
2010	50	52	74
2011	34	52	57
2012	53	56	73
2013 – erstes Halbjahr	29	32	36

7. Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung seit 2011 Ausfuhrgenehmigungen für so genannte IMSI-Catcher in welche Bestimmungsländer erteilt (Antwort auf die Schriftliche Frage 60 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 17/8102)?

Im Zeitraum vom 1. Januar 2011 bis zum 30. Juni 2013 wurden den Unternehmen Rohde & Schwarz und Syborg Informationssysteme Ausfuhrgenehmigungen für die genannten Güter in die Bestimmungsländer Argentinien, Brasilien, Indonesien, Kosovo, Malaysia, Norwegen und Taiwan erteilt.

8. Wie viele TKÜ-Maßnahmen nach richterlicher Anordnung hat das Bundeskriminalamt seit 2007 durchgeführt (bitte anders als auf Bundestagsdrucksache 17/8544 nach einzelnen Jahren aufschlüsseln und auch das erste Halbjahr 2013 aufführen)?

Jahr	TKÜ-Maßnahmen
2007	271
2008	143
2009	113
2010	142
2011	106
2012	117
2013 (bis 30.06.)	61

9. Welche Bundesbehörden betreiben an welchen Standorten und in welchen Abteilungen eigene Server zum Ausleiten bzw. Empfangen von Daten aus der Telekommunikationsüberwachung (TKÜ) durch Betreiber von Telekommunikationsanlagen?

Das BKA betreibt am Standort Wiesbaden (in der Abteilung IT) eine gemeinsam von Bundespolizei (BPOL) und BKA genutzte Telekommunikationsüberwachungsanlage (TKÜ-Anlage). Darüber hinaus betreibt das BKA (in der Abteilung KI) am Standort Wiesbaden eigene Server zum Empfang von Daten aus TKÜ-Maßnahmen.

Das ZKA in Köln sowie die Zollfahndungsämter Berlin-Brandenburg, Essen, Frankfurt/Main, Hamburg, Hannover, München und Stuttgart betreiben an ihren Hauptstandorten jeweils Server zum Empfangen der Daten aus der Telekommunikationsüberwachung. Die Anlage des Zollfahndungsamtes (ZFA) Dresden wird am Dienstsitz Görlitz betrieben. Die Server werden beim ZKA in der Gruppe II und bei den Zollfahndungsämtern jeweils im Bereich „Einsatzunterstützung“ betrieben.

Die Bundespolizei (BPOL) nutzt zum Empfang von Daten aus der Telekommunikationsüberwachung derzeit ausschließlich Server, die durch das BKA in Wiesbaden betrieben werden.

Im Hinblick auf den BND ist die Bundesregierung nach sorgfältiger Abwägung zwischen dem aus Artikel 38 Absatz 1 Satz 2 i. V. m. Artikel 20 Absatz 2 Satz 2 GG resultierenden Informationsrecht des Deutschen Bundestages einerseits und den hier vorliegenden Geheimhaltungsinteressen andererseits zu der Auffassung gelangt, dass im Rahmen einer Kleinen Anfrage eine Bekanntgabe der Telekommunikationsbeziehungen und der damit verbundenen Technikstandorte und Abteilungen im Sinne der Anfrage aus Gründen des Staatswohls nicht erfolgen kann. Hierbei waren folgende Erwägungen leitend:

Die erfragten Informationen ermöglichen Rückschlüsse auf Umfang, Struktur und Kapazitäten der strategischen Fernmeldeaufklärung des BND und damit auf einen Kernbereich der seiner Aufgabenerfüllung, insbesondere auch auf Arbeitsweisen, Strategien, Methoden und Erkenntnisstand. Dies würde die Aufgabenwahrnehmung des BND nachhaltig gefährden. Eine Weiterleitung an die Geheimschutzstelle des Deutschen Bundestages kommt nicht in Betracht, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]).

Das Informationsrecht des Deutschen Bundestages ist gleichwohl gewahrt. Im Hinblick auf die für die Durchführung von strategischen Beschränkungsmaß-

nahmen nach §§ 5 und 8 G10 auszuwählenden Telekommunikationsbeziehungen werden diese durch die zuständigen auswertenden Abteilungen des BND anhand am Aufklärungsprofil orientierter, fachlicher und technischer Erwägungen unter Berücksichtigung der gesetzlichen Vorgaben festgestellt. Die Anordnung erfolgt durch das BMI nach Maßgabe der §§ 9, 10 G10 mit Zustimmung des Parlamentarischen Kontrollgremiums gemäß § 5 Absatz 1, Satz 2 G10. Diese sehr weite Genehmigungszuständigkeit des Parlaments für exekutives Handeln gleicht die Einschränkungen beim Kreis der informationszugangsberechtigten Personen aus. Das der Bundesregierung verfassungsrechtlich auferlegte Gebot, den Deutschen Bundestag in die Lage zu versetzen, seine Aufgabe der parlamentarischen Kontrolle des Regierungshandeln effektiv wahrzunehmen (vgl. BVerfGE 124, 161 [192]), ist dadurch erfüllt. Der Gesetzgeber hat mit dem G10 eine Balance zwischen dem parlamentarischen Kontrollrecht und nachrichtendienstlichen Geheimhaltungsinteressen hergestellt, indem er der zur Gewährleistung der Geheimhaltung erforderlichen Beschränkung der Anzahl der informationszugangsberechtigten Personen weitgehende parlamentarische Kontroll- und Genehmigungsbefugnisse zur Seite gestellt hat. Die Bundesregierung ist der Auffassung, dass dadurch im Sinne praktischer Konkordanz sowohl den nachrichtendienstlichen Geheimhaltungsinteressen wie auch der parlamentarischen Kontrolle in einer Weise Rechnung getragen worden ist, die beide optimal zur Geltung kommen lässt.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

10. Welche „technische[n] Einrichtungen (Computersysteme)“ sind in der Bundestagsdrucksache 17/8544, Antwort der Bundesregierung zu Frage 4d, konkret gemeint, welche Produkte welcher Firmen werden hierfür genutzt, und welche Kosten sind für Beschaffung und Betrieb seit 2007 entstanden?

Bei den in der Antwort der Bundesregierung zu Frage 4d genannten „technischen Einrichtungen (Computersysteme)“ handelt es sich um typische Standardcomputertechnik, wie Netzwerkkarten, ISDN-Anschlusskarten, Festplatten, Storage-Arrays und Server. Hierfür kommen Standardprodukte der Firmen IBM, HP, EMC^2 und weiterer Hersteller zum Einsatz. Hinzu kommen die TKÜ-Fachanwendungen. Hierfür werden Softwarelösungen der Anbieter Syborg, DigiTask, Atis und Secunet genutzt.

Beim BKA sind hierfür seit 2007 Beschaffungskosten in Höhe von 7 863 624,08 Euro und Betriebskosten in Höhe von 2 155 982,96 Euro angefallen.

Bei der BPOL sind hierfür seit 2007 Beschaffungskosten in Höhe von 1,06 Mio. Euro und Betriebskosten in Höhe von 1,11 Mio. Euro angefallen.

Beim Zoll sind hierfür seit 2007 Beschaffungskosten in Höhe von 2 262 668,01 Euro und Betriebskosten in Höhe von 2 066 044,42 Euro angefallen.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

11. Inwiefern sind die Gesamtkosten von Auskunftsersuchen für TKÜ seit 2012 weiter gestiegen, und worin liegt der Grund für den Anstieg seit 2007 (Bundestagsdrucksache 17/8544)?

Gemäß Antwort der Bundesregierung zu Frage 3a auf Bundestagsdrucksache 17/8544 betrugen die TKÜ-Gesamtkosten für Auskunftsersuchen und TKÜ im BKA (diese wurden in der Frage 3a auf Bundestagsdrucksache 17/8544 erfragt) im Jahr 2011 396 176,48 Euro. Demgegenüber wurden in 2012 hierfür Geldmittel i. H. v. 362 096,04 Euro aufgewendet. Dies ist eine Reduzierung um rund 34 000 Euro.

12. Hält die Bundesregierung weiterhin an ihrer Aussage fest, dass Bundesbehörden keine einzelnen Metadaten in großen Internetknoten wie DE-CIX filtern, obwohl dies vom Abhördienstleister und Zulieferer deutscher Behörden Utimaco berichtet wird (Utimaco LIMS Whitepaper „Elemente einer modernen Lösung zur gesetzeskonformen Überwachung von Telekommunikationsdiensten“)?

Der Bundesregierung ist eine solche Aussage nicht bekannt.

13. Falls die Bundesregierung nicht an ihrer Aussage festhält, inwiefern und auf welche Weise wird der Internetknoten DE-CIX bzw. andere entsprechende Schnittstellen von Glasfaserkabeln durch welche Bundesbehörden überwacht?

Auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.*

14. Wie oft haben welche Bundesbehörden seit 2012 von „WLAN-Catchern“ Gebrauch gemacht, und inwiefern ist ihr Einsatz seit 2007 angestiegen?

Seitens des BKA und des Zollfahndungsdienstes wurde im Jahr 2012 jeweils einmal ein WLAN-Catcher eingesetzt. Im Jahr 2013 wurde noch kein WLAN-Catcher eingesetzt. Der Einsatz von WLAN-Catchern ist seit dem Jahr 2007 (fünf Einsätze) rückläufig.

15. Kann die Bundesregierung, obwohl sie keine Statistiken über die Anwendung der Funkzellenauswertung führen will, für ihre einzelnen Behörden zumindest Angaben über die ungefähre Größenordnung ihrer Anwendung seit 2012 (analog zu Bundestagsdrucksache 17/8544: etwa 1 bis 10 pro Jahr, 50 bis 100 pro Jahr, über 100 pro Jahr), um nachzuvollziehen, ob diese gegenüber den Angaben in der besagten Bundestagsdrucksache zu- oder abnehmen?

Durch BKA und BPOL sind seit Beginn 2012 bis heute jeweils weniger als 50 Funkzellenauswertungen durchgeführt worden. Von den Behörden der Zollverwaltung wurden im gleichen Zeitraum 93 Funkzellenauswertungen durchgeführt.

Nachrichtendienste haben keine Funkzellenauswertungen durchgeführt.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

16. Welche Funkzellenabfragen wurden dem Generalbundesanwalt beim Bundesgerichtshof seit 2012 vom Ermittlungsrichter gestattet, und im Zusammenhang mit welchen Ermittlungen fanden diese statt?

Im angefragten Zeitraum hat der Ermittlungsrichter des Bundesgerichtshofs auf Antrag des Generalbundesanwalts drei Beschlüsse mit der Anordnung erlassen, Auskunft über die Verkehrsdaten von bestimmten Funkzellen zu geben. Die Ermittlungen sind nicht abgeschlossen.

Weitere Angaben zu Zahl und Inhalt laufender bzw. konkreter Ermittlungsverfahren kann die Bundesregierung nicht machen. Trotz ihrer grundsätzlichen verfassungsrechtlichen Pflicht, Informationsansprüche des Deutschen Bundestages zu erfüllen, tritt hier nach Abwägung der betroffenen Belange das Informationsinteresse des Parlaments hinter den berechtigten Geheimhaltungsinteressen zurück. Eine weitergehende Auskunft könnte gegebenenfalls Ermittlungsmaßnahmen erschweren oder gar vereiteln, weshalb aus dem Prinzip der Rechtsstaatlichkeit folgt, dass vorliegend das betroffene Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege und Strafverfolgung (vgl. dazu BVerfGE 51, 324 (343 f.)) Vorrang vor dem parlamentarischen Informationsinteresse hat.

17. Welche weiteren Hersteller haben seit 2011 (Antwort auf die Schriftliche Frage 15 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 17/8102) an polizeiliche oder geheimdienstliche Bundesbehörden Software zur computergestützten Bildersuche bzw. zu Bildervergleichen (auch testweise) geliefert, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, bzw. welche Nutzung ist anvisiert, welche konkreten Behörden bzw. deren Abteilungen sind bzw. wären darüber zugriffsberechtigt, und in welchen Ermittlungen kommen bzw. kämen diese im Einzel- oder Regelfall zur Anwendung (bitte mit Beispielen erläutern)?

Die bisher beim BKA genutzte Software des Herstellers DotNetFabrik (vgl. Bundestagsdrucksache 17/8102, Schriftliche Frage 15 des Abgeordneten Andrej Hunko, DIE LINKE.) wurde im Jahr 2013 durch eine aktuelle Softwareversion mit dem Namen DoublePics ersetzt. Diese dient, wie auch die Vorgängerversion, dem computergestützten Abgleich von kinderpornografischen/jugendpornografischen Bilddateien im Zuständigkeitsbereich der Kriminalpolizeilichen Zentralstelle des BKA für Straftaten gegen die sexuelle Selbstbestimmung von Kindern und Jugendlichen.

Über einen Bildvergleich mit der Bildvergleichssammlung des BKA kann mittels dieser Software festgestellt werden, ob es sich um neues oder bereits bekanntes und ggf. bereits identifiziertes kinderpornografisches/jugendpornografisches Material handelt.

Abgefragte Bilder werden in der Regel in der Bildvergleichssammlung gespeichert und stehen so unmittelbar für zukünftige Abfragen bereit. Zugriffsberechtigt sind lediglich Beschäftigte des BKA, welche im Fachreferat mit der Bearbeitung von Fällen des sexuellen Missbrauchs bzw. der Verbreitung von Kinder-/Jugendpornografie beschäftigt sind.

Ein Zugriff beim Abgleich kinder-/jugendpornografischer Bilddateien auf das WWW oder sonstige Datenbanken erfolgt nicht. Der Abgleich wird ausschließlich mit Bildern der Bildvergleichssammlung durchgeführt.

Darüber hinaus wurde eine Testversion der Software PhotoDNA des Herstellers Microsoft beschafft. Im Übrigen ist im BKA das Forensic Toolkit von Access Data im Einsatz, welches in der neuen Version 5 (ab 2013) u. a. als Modul die

Software PhotoDNA von Microsoft enthält. Die Funktionalität dieses Bestandteils wurde aber noch nicht erprobt.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

18. Welche Kosten sind für Tests oder Beschaffung entsprechender Software zur computergestützten Bildersuche bzw. zu Bildervergleichen seit 2007 entstanden (bitte für die einzelnen Jahre aufschlüsseln)?

Jahr	BKA
2007	45 815,00 Euro
2008	45 815,00 Euro
2009	127 925,00 Euro
2010	32 930,00 Euro
2011	165 640,25 Euro
2012	134 771,75 Euro
2013 (bis 30.06.)	8 358,00 Euro

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

19. Auf welche Datensätze kann die Software „Cognitec“ zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, welche konkreten Behörden bzw. deren Abteilungen sind darüber zugriffsberechtigt, und inwiefern kann die Bundesregierung mitteilen, ob ihre Anwendung in den letzten Jahren zu- oder abnimmt?

Bei Cognitec handelt es sich nicht um eine Software, sondern um den Hersteller der Software „Face-VACS/DB Scan“.

BKA:

Face-VACS/DB Scan wird im BKA seit dem 13. März 2007 zum Lichtbildvergleich genutzt. Sie gleicht über einen Algorithmus die biometrischen Merkmale von Suchbildern mit den biometrischen Merkmalen der im INPOL-Bestand gespeicherten Lichtbilder – und hier nur der Portraitbilder – ab.

Die Software wird innerhalb des BKA vom Erkennungsdienst genutzt und steht über eine Verbundschnittstelle den angeschlossenen Landeskriminalämtern (LKÄ) zur Verfügung (neben dem BKA nutzen die BPOL und alle LKÄ mit Ausnahme von Bremen und Schleswig-Holstein das Gesichtserkennungssystem).

Mit der Software soll eine Identifizierung von unbekannten Personen ermöglicht werden. Ein derartiges Verfahren kommt dann zum Tragen, wenn andere Identifizierungsverfahren (Fingerabdruck, DNA) nicht möglich sind bzw. keine entsprechenden Spuren vorliegen (Subsidiarität der Gesichtserkennung).

In den Jahren 2008 bis 2011 hat die Nutzung des GES zugenommen. Ein Ausbau des Systems auf weitere Funktionen ist derzeit nicht geplant

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

BVA:

Auch das BVA setzt im Rahmen des Fundpapierverfahrens und des Visa-Verfahrens das Produkt Face-VACS/DB Scan ein.

Im Rahmen des Visumverfahrens erfolgt ein Zugriff auf die Datensätze, die aufgrund des vorherigen alphanummerischen Suchverfahrens nicht eindeutig identifiziert werden konnten. Zweck dieser Vorgehensweise ist es, nicht mehr Daten als zwingend erforderlich an die anfragende Auslandsvertretung zurückzumelden.

Die Servicestelle Fundpapierverfahren hingegen vergleicht eingehende ausländische Funddokumente mit bereits vorhandenen Datensätzen aus der Fundpapierdatenbank. In beiden Anwendungsfällen erfolgt der Zugriff durch Mitarbeiter des BVA, die unter Zuhilfenahme des Biometrie-Ergebnisses eine abschließende Zuordnungsentscheidung treffen. Eine Quantifizierung der Anwendungsfälle ist nicht möglich, da es sich um eine rein interne Zuordnungssuche handelt, die nur zur Anwendung kommt, wenn aus der alphanummerischen Suche kein eindeutiges Ergebnis hervorgeht.

Im Übrigen wird auf die Antwort zu Frage 17 und den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

20. Auf welche Datensätze kann die Software „DotNetFabrik“ zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, welche konkreten Behörden bzw. deren Abteilungen sind darüber zugriffsberechtigt, und inwiefern kann die Bundesregierung mitteilen, ob ihre Anwendung in den letzten Jahren zu- oder abnimmt?

Bei „DotNetFabrik“ handelt es sich um einen Hersteller von Software und nicht um eine Software. Von dieser wird u. a. die Bilderkennungssoftware „DoublePics“ angeboten.

Im Übrigen wird auf die Antwort zu Frage 17 verwiesen.

21. Worum handelt es sich bei der „von Interpol zur Verfügung gestellte Software im Zusammenhang mit der von Interpol eingerichteten Bilddatenbank Kinderpornografie“ (Bundestagsdrucksache 17/8102), auf welche Datensätze kann diese Software zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, welche konkreten Behörden bzw. deren Abteilungen sind darüber zugriffsberechtigt, und inwiefern kann die Bundesregierung mitteilen, ob ihre Anwendung in den letzten Jahren zu- oder abnimmt?

Die in Rede stehende ICSE DB (International Child Sexual Exploitation Database) ermöglicht in ihrer derzeitigen Ausbaustufe den Vergleich von Bilddateien sowohl basierend auf Hashwerten (1:1-Treffer) als auch auf Bildinhalten (Ähnlichkeitstreffer) im Online-Zugriff.

Die ICSE DB befindet sich seit März 2009 beim Generalsekretariat von Interpol in Lyon im Wirkbetrieb. Sie ist das Ergebnis eines G8-finanzierten Projekts.

Die Abfrage und Bestückung der Datenbank erfolgt dezentral online durch die nationalen Zentralstellen der teilnehmenden Staaten. Für Deutschland ist das Interpol Wiesbaden. Derzeit sind über 50 Staaten an die Datenbank angeschlossen.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Über die Abfrage in der Datenbank kann festgestellt werden, ob es sich um neues oder bereits bekanntes und ggf. bereits identifiziertes kinderpornografisches Material handelt. So können Doppelarbeit und vertiefte Eingriffe (zum Beispiel durch Fahndungsmaßnahmen) vermieden sowie durch die systematische Sammlung neuer Bilder und Videos in der Gesamtschau wertvolle Ermittlungsansätze gewonnen werden. Abgefragte Bilder werden in der Regel in der Datenbank mit den relevanten Falldaten angereichert und stehen so unmittelbar für zukünftige Abfragen aller anderen Staaten bereit. Der potentielle Mehrwert der ICSE DB wächst somit stetig mit der Anzahl der teilnehmenden Staaten und deren aktiven Nutzung der Datenbank.

Mit dem Anstieg der Fälle im Deliktsbereich geht automatisch auch ein Anstieg der Nutzung der Datenbank einher.

22. Auf welche Datensätze kann die Software „L1 Identity Solutions“ zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, welche konkreten Behörden bzw. deren Abteilungen sind darüber zugriffsberechtigt, und inwiefern kann die Bundesregierung mitteilen, ob ihre Anwendung in den letzten Jahren zu- oder abnimmt?

L-1 Identity Solutions ist nicht der Name einer Software, es handelt sich um einen Hersteller von biometrischen Systemen.

Die BPOL nutzt derzeit Software dieses Herstellers als Bestandteil des Grenzkontrollsystems EasyPASS. Dies dient dem Vergleich des im Chip des ePasses elektronisch gespeicherten Gesichtsbildes mit dem der Person.

Die dabei aufgenommenen Gesichtsbilder werden nicht gespeichert oder im Ermittlungsverfahren verwendet.

L-1 Identity Solutions ist Konsortialführer des vom BMBF geförderten Projektes „Multi-Biometrische Gesichtserkennung“ (GES-3D), an dem auch das BKA beteiligt ist. Derzeit wird jedoch keine Software dieser Firma im BKA genutzt.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

23. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung (bitte nach Vorgangsbearbeitung und kriminalistischer Fallbearbeitung aufschlüsseln), bzw. inwiefern haben sich gegenüber der Bundestagsdrucksache 17/8544 hierzu Änderungen, insbesondere zu genutzten „Zusatzmodulen“ ergeben?

Es haben sich keine Änderungen im Vergleich zur Bundestagsdrucksache 17/8544, Antworten zu den Fragen 14 ff. ergeben.

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

24. Welche Kosten sind den Bundesbehörden im Einzelfall und unter Berücksichtigung der Arbeitszeit innerhalb der Behörde für die Beschaffung, Anpassung, den Service und die Pflege der Software gegenüber der Aufstellung auf Bundestagsdrucksache 17/8544 seit 2012 entstanden?

Vorbemerkung:

Die Kosten für die Arbeitszeit von Mitarbeitern der Bundesbehörden können mangels hierzu geführter Statistiken nicht erhoben werden.

BPOL:

Gegenüber der Bundestagsdrucksache17/8544 entstanden für die Jahre 2012/2013 bei der BPOL folgende Kosten für Service/Wartung/Pflege/Anpassungen:

Anwendung	Kosten 2012	Kosten 2013
@rtus-Bund	723 517,67 Euro	850 850,00 Euro
b-case	425 359,92 Euro	319 019,94 Euro

BKA:

Für das Fallbearbeitungssystem b-case sind für Wartung, Pflege und Lizenzerweiterung im Rahmen der Gemeinsamen Ermittlungsdatei – Zwischenlösung (GED) Kosten in Höhe von 1 436 000 Euro angefallen.

Für die Entwicklung des Kriminaltechnischen Informationssystems (KISS), inkl. aller Module, des Forensischen Informationssystems Handschriften (FISH-neu) und des Kriminaltechnischen Informationssystems Texte (KISTE) sind für Entwicklung, Weiterentwicklung und Pflege ab 1998 insgesamt ca. 1,4 Mio. Euro angefallen, davon 155 000 Euro im Zeitraum ab dem Jahr 2012.

Die Kosten, die für das intern entwickelte Fallbearbeitungssystem (INPOL-Fall) und das Vorgangsbearbeitungssystem (VBS) seit 2012 angefallen sind und die hauptsächlich auf internen Entwicklungsarbeiten basieren, können mangels hierzu geführter Statistiken nicht erhoben werden.

Zollverwaltung:

Im Zollfahndungsdienst sind für Beschaffung, Anpassung, den Service und die Pflege des Systems INZOLL im Jahr 2012 Kosten in Höhe von 448 409,05 Euro und im Jahr 2013 bisher 273 739,03 Euro, also insgesamt seit 2012 722 148,08 Euro angefallen.

Die Weiterentwicklung, Wartung und Pflege des IT-Verfahrens ProFiS der FKS erfolgt durch das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT). Die Kosten hierfür beliefen sich im Jahr 2012 auf ca. 640 000 Euro und im Jahr 2013 auf ca. 322 000 Euro.

25. Welche weiteren Produkte der Firma rola Security Solutions (auch Zusatzmodule) wurden seit 2012 für welche Behörden und welche Einsatzzwecke beschafft, und welche neueren Errichtungsanordnungen existieren für deren Einsatz?

Das BKA hat seit 2012 keine weiteren Produkte der Firma rola Security Solutions GmbH beschafft. In 2012 wurden jedoch folgende Module für das Fallbearbeitungssystem b-case beauftragt:

– Kennzeichnungspflicht

– Mapping-Tool für Bund-Länder-Datei-Schnittstelle (BLDS)

– Antiterrordatei-Schnittstellenerweiterung für das Datenabgleichsverfahren (DAV)

– Mapping- und Administrationsanpassung BLDS

Die BPOL hat seit 2012 folgende Zusatzmodule/Schnittstellen abschließend beschafft, Änderungen der Errichtungsanordnungen waren hierfür nicht erforderlich:

– Text Link

– BLOS Datenübernahme

– IMP/FTS Suche/Datenaustausch

– Info- und Störungsanzeige für fachliche Administratoren

– Mapping Tool für Schnittstellen incl. Adapter

– Modul für Kennzeichnungspflichten

Der BND hat seit 2012 keine Produkte der Firma rola Security Solutions beschafft.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

26. Inwiefern und wofür werden Anwendungen von rola Security Solutions auch bei In- und Auslandsgeheimdiensten der Bundesregierung genutzt?

Hierzu wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

27. Welche neueren Details kann die Bundesregierung zur endgültigen Einrichtung des Kompetenzzentrums Informationstechnische Überwachung (CC ITÜ) mitteilen?

Das „Kompetenzzentrum Informationstechnische Überwachung“ (CC ITÜ) wurde im September 2012 in Form einer neuen Gruppe im BKA eingerichtet, welche sich aus drei Fachbereichen zusammensetzt. Im Fachbereich „Softwareentwicklung und -pflege ITÜ“ werden die BKA-eigene Software zur Durchführung von Maßnahmen der Quellen-TKÜ entwickelt sowie die im BKA eigenentwickelte Software zur Durchführung von Maßnahmen der Online-Durchsuchung fortentwickelt und für den jeweiligen Einsatzfall bereitgestellt. Die Durchführung von Maßnahmen der TKÜ/ITÜ einschließlich der erforderlichen netzwerkforensischen Untersuchungen der dabei gewonnen Daten erfolgt im Fachbereich „Einsatz und Service TKÜ/ITÜ“. Der Fachbereich „Monitoring, Test und Protokollierung ITÜ“ ist für die Gewährleistung der rechtskonformen Entwicklung und des rechtskonformen Einsatzes einschließlich der Protokollierung des Einsatzes von Software zur Durchführung von Maßnahmen informationstechnischer Überwachung zuständig (Qualitätssicherung).

Die vom Haushaltsausschuss des Deutschen Bundestages bewilligten zusätzlichen 30 Planstellen für die Bereiche „Softwareentwicklung und -pflege“ sowie „Monitoring, Test und Protokollierung“ des CC ITÜ konnten zwischenzeitlich im Rahmen von internen und externen Personalgewinnungsmaßnahmen bis auf fünf Stellen besetzt werden.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

28. In welcher Höhe ist das CC ITÜ im Jahr 2013 mit Finanzmitteln ausgestattet worden, und wie ist der Haushaltansatz für das Jahr 2014?

In 2013 wurde das CC ITÜ mit Sachmitteln in Höhe von 419 000 Euro aus dem Haushalt des BKA ausgestattet. Zusätzlich stehen im Haushaltsjahr 2013 noch Restmittel aus dem Sondertatbestand 2012 (siehe Antwort zu Frage 29) zur Verfügung. Der Haushaltsansatz für das Jahr 2014 steht noch nicht fest.

29. Wie verteilen sich die Finanzmittel für die Beschaffung bzw. Programmierung von Computerspionageprogrammen (staatliche Trojaner) sowie andere Soft- und Hardware zur „informationstechnischen Überwachung“, und um welche Anwendungen handelt es sich dabei konkret?

Das BKA entwickelt bzw. beschafft zur rechtmäßigen Durchführung von Maßnahmen der informationstechnischen Überwachung im Rahmen der Strafverfolgung bzw. Gefahrenabwehr Überwachungssoftware nach Maßgabe der gesetzlichen Befugnisse. Das BKA distanziert sich daher von einer Verwendung der Begriffe Computerspionageprogramme bzw. staatliche Trojaner.

Primär für die Eigenentwicklung (Programmierung) einschließlich der entsprechenden Qualitätssicherung einer Quellen-TKÜ-Software wurden dem BKA auf Beschluss des Haushaltsausschusses des Deutschen Bundestages in 2012 2,2 Mio. Euro Sachmittel als Sondertatbestand zur Verfügung gestellt. Die Beschaffung der kommerziellen Quellen-TKÜ-Software der Fa. Gamma International GmbH als Übergangslösung erfolgt ebenfalls mit HH-Mitteln aus diesem Sondertatbestand aus dem Jahr 2012.

2013 stehen dem CC ITÜ ausschließlich die in der Antwort zu Frage 28 aufgeführten Haushaltsmittel zur Verfügung. Bei der darüber hinaus beschafften Soft- und Hardware handelt es sich um technische Mittel, welche bei verschiedenen Maßnahmen der IuK-gestützten Einsatz-/Ermittlungsunterstützung eingesetzt werden, so dass eine Separierung der ausschließlich für den Bereich der informationstechnischen Überwachung beschafften Sachmittel nicht möglich ist.

30. Welche Akteure (Ämter, Behörden, Institute, Firmen, Stiftungen etc.) werden in deren Entwicklung und Anwendung eingebunden?

Beschäftigte der LKÄ Bayern und Hessen sowie des ZKA sind unterstützend im CC ITÜ eingebunden (vgl. Antwort zu Frage 19, Bundestagsdrucksache 17/10944). Zwischenzeitlich hat auch das Landeskriminalamt Baden-Württemberg einen Mitarbeiter in das CC ITÜ entsandt.

Im Zusammenhang mit der Eigenentwicklung einer Software zur Durchführung von Maßnahmen der Quellen-TKÜ nehmen die Firmen CSC Deutschland Solutions GmbH und 4Soft eine unterstützende und beratende Funktion wahr, ohne in das CC ITÜ organisatorisch eingebunden zu sein.

31. Was ergab die Prüfung des Quellcodes beschaffter Trojaner-Programme, und welche Schlüsse zieht die Bundesregierung daraus?

Die kommerzielle Quellen-TKÜ-Software der Fa. Gamma International GmbH entspricht in der bisher vorliegenden Version noch nicht vollständig den Vorgaben und Anforderungen der Standardisierenden Leistungsbeschreibung (SLB). Derzeit werden durch den Hersteller entsprechende Anpassungen der Software vorgenommen, die nach Fertigstellung einer fortgesetzten Quellcode-Prüfung zu unterziehen sind. Ein Einsatz der Software kommt nur in Betracht, wenn die vollständige Konformität mit der SLB hergestellt ist.

32. Wie ist eine Kontrolle des CC ITÜ inzwischen vorgesehen, und welche Rolle spielt das auf Bundestagsdrucksache 17/8544 angegebene „Expertengremium“?

Im Rahmen der üblichen Kontrollfunktionalität unterliegt das CC ITÜ der Fachaufsicht des BMI. Das in der Antwort zu Frage 23d in der Bundestagsdrucksache 17/8544 angeführte „Expertengremium“ wurde nicht eingerichtet. Das mit diesem Expertengremium verfolgte Ziel, der Prüfung der Standardisierenden Leistungsbeschreibung im Hinblick auf Aspekte der Datenschutzes und der Informationssicherheit, wurde durch die enge Einbindung beider Stellen im Rahmen ihrer gesetzlichen Aufgaben erreicht.

33. Welche Software zur Überwachung, Ausleitung, Analyse und Verarbeitung ausgeforschter digitaler Kommunikation kommt bei den In- und Auslandsgeheimdiensten der Bundesregierung zur Anwendung, und welche Angaben kann die Bundesregierung zu deren Funktionsweise machen?

Hierzu wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

34. Welche Bundesbehörden haben in der Vergangenheit welche Geschäfte mit der Gesellschaft für technische Sonderlösungen KG (GTS) sowie der AIM GmbH getätigt (bitte die Produkte und deren Funktionalität angeben)?

Im Zusammenhang mit der Beschaffung der Software „Netwitness Investigator“ hat das BKA in der Vergangenheit Geschäftsbeziehungen mit den Firmen GTS und ALM GmbH unterhalten. Das BKA setzt die Software „Netwitness Investigator“ ausschließlich als forensisches Analysewerkzeug zur Untersuchung/Auswertung von bereits erhobenen Daten ein, jedoch nicht zur Aufzeichnung solcher Daten.

Im Übrigen wird auf den VS-Geheim eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

35. Welche Bundesbehörden haben in der Vergangenheit welche Geschäfte mit welchen anderen Firmen des Geschäftsführers der Gesellschaft für technische Sonderlösungen (GTS) getätigt (bitte die Produkte und deren Funktionalität angeben)?

Es bestanden keine sonstigen geschäftlichen Beziehungen zu anderen Firmen des Geschäftsführers der GTS.

36. Bei welchen Behörden wird die Software „Netwitness“ bzw. vergleichbare Anwendungen der gleichen Firma, die unter anderem Namen vermarktet werden, eingesetzt, auf welche Datensätze wird dabei zugegriffen, und nach welchen Verfahren werden diese durchsucht (Bundestagsdrucksache 17/8544)?

Auf die Antwort zu Frage 34 sowie auf den VS-Geheim eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung wird verwiesen.*

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

37. Inwiefern treffen Berichte zu, dass Produkte der Firmen Narus und Polygon sowie die Software „X-Keyscore“ eingesetzt werden (Magazin FAKT, 16. Juli 2013/Süddeutsche Zeitung, 21. Juli 2013)?

Die Sicherheitsbehörden des Bundes setzten keine Produkte der Firmen Narus und Polygon ein.

Im Übrigen wird auf die in Veröffentlichung befindlichen Antworten der Bundesregierung zu den Fragen 64 ff. auf Bundestagsdrucksache 17/14456 verwiesen.

38. Inwiefern treffen Berichte zu, wonach der Bundesnachrichtendienst (BND) von der US-amerikanischen NSA den Quellcode zum Abhörprogramm „Thin Thread“ bzw. einer vergleichbaren Anwendung erhielt (http://netzpolitik.org/2013/nsa-whistleblower-william-binney-bnd-erhielt-von-nsa-quellcode-des-abhor-und-analyseprogramms-thinthread/), und über welche Besonderheiten verfügt die Software?

„Thin Thread“ wurde dem BND erst durch die Presseberichterstattung bekannt. Ein Quellcode dieser Software liegt nicht vor.

39. Welchen Zwecken dient nach Kenntnis der Bundesregierung der Einsatz von Produkten der Firmen Narus und Polygon sowie der Software „X-Keyscore“ und „Thin Thread“, und auf welche Datensätze wird über welche Kanäle zugegriffen?

40. Welche Funktionsweise haben die Anwendungen?

Auf die Antworten zu den Fragen 37 und 38 wird verwiesen.

41. Inwieweit befassen sich auch die Treffen der Gruppe der Sechs (G6), an denen auf Betreiben des damaligen Bundesinnenministers Dr. Wolfgang Schäuble seit dem Jahr 2006 auch die USA teilnehmen, mit der geheimdienstlichen Überwachung der Telekommunikation?

Zum so genannten G6-Treffen der Innenminister werden erst seit 2007 auch die Minister für Innere Sicherheit und für Justiz der USA zu Sicherheitsthemen eingeladen. Dem liegt die Überzeugung zugrunde, dass man den internationalen Bedrohungen der Sicherheit, insbesondere durch Terrorismus, durch eine transatlantische Zusammenarbeit besser begegnen kann. Geheimdienstliche Fragen werden in diesem Rahmen aber nicht besprochen.

42. Welchen Inhalt hatte das „EU-US Law-enforcement Meeting“ vom 15./16. April 2013, und welche Personen der Bundesregierung oder anderer deutscher Einrichtungen nahmen mit welchen Beiträgen daran teil?

43. Welche Themen wurden diskutiert, und wer hatte diese jeweils vorgeschlagen bzw. vorbereitet?

44. Welche Ergebnisse bzw. welcher Zwischenstand folgte aus den Beratungen und Diskussionen?

Die Fragen 42 bis 44 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

An dem EU-US Law-enforcement Meeting nahmen keine deutschen Behördenvertreter teil. Der Bundesregierung liegen daher keine eigenen Erkenntnisse zu der Veranstaltung vor.

Auf die Antwort der Kommissarin Malmström auf die parlamentarische Anfrage der Abgeordneten des Europäischen Parlaments Sabine Lösing vom 24. Juli 2013, die unter www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2013-005923+0+DOC+XML+V0//DE abgerufen werden kann, wird ergänzend hingewiesen.

45. Welche Treffen zwischen welchen Behörden der USA und der Bundesregierung haben 2012 und 2013 auf Ministerebene bzw. zwischen Staatssekretären stattgefunden, in denen die geheimdienstliche Überwachung der Telekommunikation bzw. der Austausch daraus folgender Erkenntnisse erörtert wurde, wann fanden die Treffen statt, und welches Ergebnis zeitigten diese?

Im Jahr 2012 fanden keine solchen Treffen statt. Für das Jahr 2013 wird auf die in Veröffentlichung befindlichen Antworten der Bundesregierung zu den Fragen 7, 8, 9 und 10 auf Bundestagsdrucksache 17/14456 sowie die Vorbemerkung der Bundesregierung hierzu verwiesen.

46. Welche ausländischen und deutschen Behörden sowie sonstige deutschen Teilnehmerinnen/Teilnehmer haben nach Kenntnis der Bundesregierung am Treffen der „Hochrangigen Expertengruppe“ (EU/US High level expert group) am 22. und 23. Juli 2013 in Vilnius teilgenommen, und welche aus Sicht der Bundesregierung besonderen Ergebnisse zeitigte die Veranstaltung?

Wann und wo finden welche Folgetreffen statt?

Die Europäische Kommission und die EU-Präsidentschaft haben die von den Mitgliedstaaten benannten Experten, die allein als Experten zur Beratung der Co-Chairs teilgenommen haben, gebeten, Berichte zu dieser Expertengruppe ausschließlich der EU-Kommission, der EU-Präsidentschaft und dem Ausschuss der Ständigen Vertreter (AStV) vorzubehalten. Deutschland respektiert diesen Wunsch für die Übergangszeit bis zur Vorlage des Berichts der Europäischen Kommission, der EU-Präsidentschaft bzw. dem AStV.

47. Inwiefern entspricht die Aussage des Bundesinnenministers, dass es ein „Supergrundrecht“ auf Sicherheit gebe, auch der Haltung der Bundesregierung (DIE WELT, 16. Juli 2013)?

Dem Bundesverfassungsgericht zufolge ist die vom Staat zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit ein Verfassungswert, der mit den Grundrechten in einem Spannungsverhältnis steht. Die daraus abgeleitete Schutzpflicht findet ihren Grund sowohl in Artikel 2 Absatz 2 Satz 1 als auch in Artikel 1 Absatz 1 Satz 2 GG (BVerfGE 120, 274, 319).

Grundrechte sind in erster Linie Abwehrrechte gegen den Staat. Sie sichern die Freiheitssphäre des einzelnen vor Eingriffen der öffentlichen Gewalt. Allgemeininteressen, denen Grundrechtseingriffe dienen, sind in der konkreten Abwägung stets mit den betroffenen Individualinteressen abzuwägen.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333