

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte,
Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/3905 –**

Einsätze von sogenannten stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im zweiten Halbjahr 2014

Vorbemerkung der Fragesteller

Berichte über die zunehmende Überwachung und Analyse digitaler Verkehre untergraben das Vertrauen in die Freiheit des Internets und der Telekommunikation. Aus Antworten der Bundesregierung aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz „Stiller SMS“, sogenannter WLAN-Catcher und IMSI-Catcher nimmt stetig zu, die Ausgaben für Analysesoftware steigen ebenfalls (Bundestagsdrucksache 18/2257). Das Bundeskriminalamt hat zwei verschiedene Trojaner entwickelt und nutzt zeitgleich eine „Übergangslösung“. Der Trojaner zur „Online-Durchsuchung“ kompletter Rechnersysteme befindet sich in „Einsatzbereitschaft“ (Schriftliche Fragen 22 und 23 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/2352). Ein weiteres System zum ferngesteuerten Abhören von verschlüsselter Internettelefonie werde noch erprobt. Damit verfügt die Behörde über mindestens drei verschiedene Trojaner. An deren Entwicklung sind neben den Firmen CSC Deutschland GmbH und 4Soft GmbH auch der Münchner Überwachungsspezialist ELAMAN GmbH beteiligt. Viele weitere Details bleiben aber offen, andere sind gegenüber der Öffentlichkeit als geheim eingestuft. Es ist beispielsweise unklar, in welchem Umfang der Bundesnachrichtendienst oder die Zollkriminalämter Trojaner einsetzen. 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 anlasslos den Telekommunikationsverkehr und durchsuchen diesen nach Schlüsselbegriffen. Der frühere Bundesminister des Innern, Dr. Hans-Peter Friedrich, rechtfertigte dies damit, dass es ein „Supergrundrecht“ auf Sicherheit gebe (Bundestagsdrucksache 17/14714). Die Fragesteller erinnern demgegenüber daran, dass das Grundgesetz kein Grundrecht auf Sicherheit kennt, und sind zudem der Auffassung, dass Grundrechte nicht hierarchisiert werden können. Um das gestörte Vertrauen in das Fernmeldegeheimnis wiederherzustellen, fordern die

Fragesteller weiterhin die Veröffentlichung entsprechender Informationen, darunter auch 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 1, 2, 3, 6, 7, 10 und 11 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 von der Kleinen Anfrage betroffenen Behörden und insbesondere mit deren Aufklärungsaktivitäten und Analysemethoden stehen.

Der Schutz vor allem der technischen Aufklärungsfähigkeiten der von der Kleinen Anfrage betroffenen Behörden, insbesondere der Nachrichtendienste, stellt für deren Aufgabenerfüllung einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität ihrer Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten. Eine Veröffentlichung von Einzelheiten solcher Fähigkeiten würde zu einer wesentlichen Schwächung der ihnen zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für deren Auftrags Erfüllung 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. Die Antworten zu den Fragen 3, 6, 10, 11 sind daher gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „Geheim“ eingestuft und liegen der Geheimschutzstelle des Deutschen Bundestages vor.

Die Antworten auf die Kleine Anfrage enthalten weiterhin Angaben zu operativen Fähigkeiten und Methoden nachrichtendienstlicher Tätigkeit. Deren Kenntnisnahme durch Unbefugte könnte für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind einzelne Informationen gemäß der VSA als „VS – Vertraulich“ eingestuft. Dies betrifft teilweise die Antworten zu den Fragen 7 bis 7d. Diese liegen der Geheimschutzstelle des Deutschen Bundestages vor.

Die Antworten auf die Kleine Anfrage beinhalten darüber hinaus zum Teil detaillierte Einzelheiten zu den technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen der Behörden. Aus ihrem Bekanntwerden könnten Rückschlüsse auf den Modus Operandi, die Fähigkeiten und Methoden der Ermittlungsbehörden gezogen werden.

Deshalb sind einzelne Informationen gemäß der VSA als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt. Dies betrifft im Einzelnen ganz oder teilweise die Antworten zu den Fragen 1, 2, 3, 7 und 10.

1. Wie oft haben welche Bundesbehörden im zweiten Halbjahr 2014 von WLAN-Catchern Gebrauch gemacht?
 - a) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?
 - b) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
 - d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Die Fragen 1, 1a, 1b und 1d werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Mit Ausnahme des als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den verwiesen wird, haben sonstige Bundesbehörden keine WLAN-Catcher eingesetzt.¹

- c) Welche Hard- und Software wird hierfür genutzt, und welche Änderungen haben sich hierzu gegenüber dem Vorjahr ergeben (Bundestagsdrucksachen 17/14714 und 18/2257)?

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 1c auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen. Gegenüber dem ersten Halbjahr 2014 haben sich keine Änderungen ergeben.

2. Welche Bundesbehörden haben im zweiten Halbjahr 2014 wie oft IMSI-Catcher eingesetzt?
 - a) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
 - b) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?

Die Fragen 2, 2a und 2b werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Das Bundeskriminalamt (BKA) setzte im zweiten Halbjahr 2014 in 14 Ermittlungsverfahren sowie in einem Zielfahndungsverfahren einen IMSI-Catcher ein. Es waren insgesamt 22 Personen betroffen.

Die Bundespolizei (BPOL) hat im zweiten Halbjahr 2014 in 25 Fällen einen IMSI-Catcher eingesetzt. Über die Anzahl betroffener Personen und der Ermittlungsverfahren liegen keine Angaben vor, da diese nicht statistisch erfasst werden.

Die Zollverwaltung (Zoll) hat in 25 Fällen IMSI-Catcher eingesetzt. Von diesen Maßnahmen waren insgesamt 25 Personen betroffen.

In Umsetzung von Beschlüssen des Ermittlungsrichters des Bundesgerichtshofes wurden im zweiten Halbjahr 2014 insgesamt achtmal IMSI-Catcher in acht Ermittlungsverfahren gegen acht Beschuldigte eingesetzt.

Mit Ausnahme des als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den verwiesen wird, haben sonstige Bundesbehörden keine IMSI-Catcher eingesetzt.¹

¹ Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Im Bereich von Maßnahmen der Strafverfolgung der Polizeien und des Zollfahndungsdienstes obliegt die Benachrichtigung von Betroffenen der zuständigen Staatsanwaltschaft. Bei den erwähnten Maßnahmen auf der Grundlage von Beschlüssen des Ermittlungsrichters des Bundesgerichtshofes handelt es sich in vier Fällen um laufende Ermittlungsverfahren, bei denen die gesetzliche Frist noch nicht abgelaufen ist, so dass die Betroffenen bisher nicht benachrichtigt worden sind.

In den übrigen vier Fällen steht derzeit noch die Gefährdung des Ermittlungszwecks einer Benachrichtigung entgegen.

Zu Benachrichtigungen bei sonstigen Maßnahmen der Strafverfolgung sowie zu Benachrichtigungen in sonstigen Fällen liegen der Bundesregierung keine statistischen Informationen vor.

- c) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Der Einsatz eines IMSI-Catchers zur Ermittlung der Gerätenummer eines Mobilfunkendgerätes und der Kartenummer der darin verwendeten Karte sowie des Standortes eines Mobilfunkgerätes darf nach § 100i der Strafprozessordnung (StPO) von dem zuständigen Gericht nur angeordnet werden, wenn dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der beschuldigten Person erforderlich ist und der Verdacht des Vorliegens einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht. Die Ermittlung der Kommunikationsmittel und der Aufenthaltsorte der Täter oder Teilnehmer einer solchen Straftat wird grundsätzlich als wesentlich eingeschätzt.

Darüber hinaus wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuftent Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.²

- d) Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung im zweiten Halbjahr 2014 Ausfuhrgenehmigungen für so genannte IMSI-Catcher in welche Bestimmungsländer erteilt?

Im zweiten Halbjahr 2014 wurde dem Unternehmen Syborg Informationssysteme eine Ausfuhrgenehmigung für die genannten Güter nach Montenegro erteilt.

3. Wie viele Maßnahmen zur Telekommunikationsüberwachung (TKÜ-Maßnahmen) hat das Bundeskriminalamt im zweiten Halbjahr 2014 durchgeführt?

Das BKA hat im zweiten Halbjahr 2014 551 TKÜ-Maßnahmen durchgeführt (diese Angabe bezieht sich auf TKÜ-Maßnahmen, die im zweiten Halbjahr 2014 begonnen wurden).

- a) Welche Bundesbehörden betreiben an welchen Standorten und in welchen Abteilungen eigene Server zum Ausleiten bzw. Empfangen von Daten aus der TKÜ durch Betreiber von Telekommunikationsanlagen,

² Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 3a auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen. Gegenüber dem ersten Halbjahr 2014 haben sich – mit Ausnahme des als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den insoweit verwiesen wird – keine Änderungen ergeben.³

- b) Welche Gesamtkosten von Auskunftersuchen für TKÜ sind im zweiten Halbjahr 2014 entstanden – soweit rekonstruierbar?

Mit Ausnahme des Inhalts des als „VS – Geheim“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den hiermit verwiesen wird, kann die Bundesregierung keine Angaben machen, da keine systematische Erfassung von Kosten im Sinne der Frage erfolgt.⁴

- c) Welche Software zur Überwachung, Ausleitung, Analyse und Verarbeitung ausgeforschter digitaler Kommunikation kommt bei den Polizeien des Bundes sowie den In- und Auslandsgeheimdiensten der Bundesregierung zur Anwendung, und welche Angaben kann die Bundesregierung zu deren Funktionsweise machen, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Zur Erfassung und Aufbereitung der im Rahmen einer Telekommunikationsüberwachung aufgezeichneten Daten nutzen die Strafverfolgungsbehörden der Zollverwaltung integrierte Fachanwendungen der Firma DigiTask GmbH (DigiTask Lawful Interception Center), vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. „Computergestütztes Aufspüren von unerwünschtem Verhalten im öffentlich Raum“ auf Bundestagsdrucksache 18/707 vom 5. März 2014.

Darüber hinaus haben sich gegenüber der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 3c auf Bundestagsdrucksache 18/2257 vom 1. August 2014 keine Änderungen ergeben.

4. Inwiefern und auf welche Weise wird der Internetknoten DE-CIX bzw. andere in Deutschland oder auch im Ausland befindliche, internationale Schnittstellen von Glasfaserkabeln durch welche Bundesbehörden überwacht, bzw. welche Änderungen haben sich hierzu ergeben (Bundestagsdrucksachen 17/14714 und 18/2257)?

Es haben sich keine Änderungen gegenüber den Angaben zum ersten Halbjahr 2014 in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014 ergeben.

³ Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

⁴ 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.

5. Wie viele Maßnahmen der Funkzellenauswertung haben welche Bundesbehörden im zweiten Halbjahr 2014 vorgenommen (bitte wie auf Bundestagsdrucksache 17/14714 beantworten)?

Das BKA hat im zweiten Halbjahr 2014 sieben Funkzellenabfragen durchgeführt.

Die BPOL hat im zweiten Halbjahr 2014 weniger als 50 Funkzellenabfragen durchgeführt.

Durch Behörden des Zollfahndungsdienstes wurden im zweiten Halbjahr 2014 27 Funkzellenauswertungen durchgeführt.

Sonstige Bundesbehörden haben im anfragegegenständlichen Zeitraum keine Funkzellenauswertung durchgeführt.

- a) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen?

Beim BKA waren fünf Personen und vier Ermittlungsverfahren betroffen. Für die übrigen Behörden liegen keine Angaben vor, da diese dort nicht statistisch erfasst werden.

- b) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

Der Bundesregierung liegen dazu keine statistischen Informationen vor.

- c) Welche Funkzellenabfragen wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof gestattet, und im Zusammenhang mit welchen Ermittlungen fanden diese statt?

Im erfragten Zeitraum wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof (GBA) keine Funkzellenabfragen angeordnet.

- d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?

Eine Funkzellendatenerhebung darf nach § 100g Absatz 2 Satz 2 StPO von dem zuständigen Gericht nur angeordnet werden, wenn der Verdacht des Vorliegens einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Ermittlung der Kommunikationsmittel und der Aufenthaltsorte der Täter oder Teilnehmer einer Straftat von erheblicher Bedeutung wird in diesen Fällen grundsätzlich als wesentlich eingeschätzt.

6. Inwiefern sind die Bundesministerien des Innern, der Verteidigung, der Finanzen oder das Bundeskanzleramt mittlerweile in der Lage, Mikrofone von Mobiltelefonen aus der Ferne zu aktivieren, um diese als Abhöreinrichtungen zu nutzen, in welchem Umfang wird dies bereits genutzt, und welche Soft- oder Hardware wird hierfür genutzt, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es wird auf den als „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen. Darüber hinaus haben sich keine Änderungen gegenüber dem ersten Halbjahr 2014 (siehe Antwort der Bundesregie-

zung zu Frage 6 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014) ergeben.⁵

7. Welche weiteren Hersteller haben im zweiten Halbjahr 2014 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, in welchen Ermittlungen kommen bzw. kämen diese im Einzel- oder Regelfall zur Anwendung, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es wird auf die Antwort der Bundesregierung zu Frage 7 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen. Gegenüber dem ersten Halbjahr 2014 haben sich – mit Ausnahme des als „VS – Nur für den Dienstgebrauch“ sowie des als „VS – Vertraulich“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den insoweit verwiesen wird – keine Änderungen ergeben.⁶

- a) Welche Kosten sind für Tests oder die Beschaffung entsprechender Software entstanden?

Es wird auf den als „VS – Vertraulich“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.⁷

Darüber hinaus sind keine diesbezüglichen Kosten entstanden, da keine entsprechenden Tests oder Beschaffungen durchgeführt wurden.

- b) Auf welche Datensätze kann die etwaige, neu beschaffte Software zugreifen, nach welchem Verfahren funktioniert diese, wo wird diese jeweils genutzt, welche konkreten Behörden bzw. deren Abteilungen sind darauf zugriffsberechtigt?

Es haben sich keine Änderungen gegenüber den Angaben zum ersten Halbjahr 2014 auf die Antwort der Bundesregierung zu Frage 7b der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014 ergeben.

- c) Inwiefern kann die Bundesregierung mitteilen, ob die Anwendung von Software zur computergestützten Bildersuche bzw. zu Bildervergleichen im Vergleich zum Vorjahr zu- oder abnimmt?

Hierzu liegen der Bundesregierung keine statistischen Daten vor. Gleichwohl führen nach Einschätzung der Bundesregierung vor allem im Phänomenbereich der Kinder- und Jugendpornografie steigende Kapazitäten bei digitalen Speichermedien kombiniert mit dem tätertypischen „Sammelverhalten“ zu einer stetig ansteigenden Anzahl der in der Zentralstelle zur Bekämpfung von Sexualdelikten zum Nachteil von Kindern und Jugendlichen pro Einzelfall auszuwer-

⁵ 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 Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

⁷ Das Bundesministerium des Innern hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

tenden Bilddateien. Neben diesem Anstieg der Anzahl der Bilder im Einzelfall ist ein kontinuierlicher Anstieg der Fallzahlen festzustellen, sodass im Ergebnis die Anzahl der Bildabgleiche pro Jahr steigend ist.

Im Übrigen wird auf den als „VS – Vertraulich“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.⁸

- d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen bzw. inwiefern lässt sich dies überhaupt rekonstruieren?

Der Abgleich von kinder- und jugendpornografischen Dateien ist im Rahmen der polizeilichen Strafverfolgung unverzichtbarer Bestandteil der Sachbearbeitung und ist grundsätzlich in allen Vorgängen durchzuführen, in denen kinder- und jugendpornografisches Material festgestellt wurde. Über die Abfrage in der Bildvergleichssammlung kann festgestellt werden, ob es sich um neues oder bereits bekanntes und ggf. bereits identifiziertes kinder- und jugendpornografisches Material handelt. So können Doppelarbeit, unnötige Eingriffe (zum Beispiel durch Fahndungsmaßnahmen) und eine erneute Viktimisierung der Opfer vermieden werden.

8. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung (bitte nach Vorgangsbearbeitung, kriminalistische Fallbearbeitung aufschlüsseln), bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 8 auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen.

- a) 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 im zweiten Halbjahr 2014 entstanden?

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

BKA:

Kosten für das Fallbearbeitungssystem INPOL-Fall und das Vorgangsbearbeitungssystem VBS werden nicht statistisch erfasst und können daher nicht beziffert werden. Im zweiten Halbjahr 2014 sind für das Fallbearbeitungssystem b-case Kosten in Höhe von ca. 298 000 Euro und für das Vorgangsbearbeitungssystem KISS Kosten in Höhe von ca. 700 000 Euro entstanden.

BPOL:

Im zweiten Halbjahr 2014 sind bei der BPOL für die Beschaffung, Anpassung, den Service und die Pflege von @rtus Bund 410 136 Euro und für b-case 354 766 Euro entstanden.

⁸ Das Bundesministerium des Innern hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Zoll:

Im Zollfahndungsdienst sind für die Beschaffung, Anpassung, den Service und die Pflege des IT-Systems INZOLL im zweiten Halbjahr 2014 Kosten in Höhe von 465 612 Euro angefallen.

Für die Beschaffung, Anpassung, den Service und die Pflege des IT-Systems ZenDa-ProFiS der Finanzkontrolle Schwarzarbeit sind im zweiten Halbjahr 2014 insgesamt 573 255 Euro angefallen.

- b) Welche weiteren Produkte der Firma rola Security Solutions GmbH (auch „Zusatzmodule“) wurden für welche Behörden und welche Einsatzzwecke beschafft, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Im Oktober 2014 erteilte das Beschaffungsbüro des Bundesministeriums des Innern den Zuschlag im Vergabeverfahren zum Aufbau der Zentralkomponente des Polizeilichen Informations- und Analyseverbands – Operativ-zentral beim BKA an die Firma rola Security Solutions.

Die BPOL hat verschiedene Einsatzfunktionalitäten beschafft, die zur Anlieferung an den Polizeilichen Informations- und Analyseverbund – Operativ-zentral dienen. Darüber hinaus wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE zu Frage 8b auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen.

- c) Inwiefern und wofür werden Anwendungen von der Firma rola Security Solutions GmbH auch bei In- und Auslandsgeheimdiensten der Bundesregierung genutzt, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es haben sich keine Änderungen gegenüber den Angaben zum ersten Halbjahr 2014 in der Antwort der Bundesregierung zu Frage 8c der Kleinen Anfrage der Fraktion DIE LINKE auf Bundestagsdrucksache 18/2257 vom 1. August 2014 ergeben.

- 9. Welche neueren Details kann die Bundesregierung zur Einrichtung des Kompetenzzentrums Informationstechnische Überwachung (CC ITÜ), dort eingesetztem Personal, Aufgabenbereichen oder Finanzmitteln mitteilen (Bundestagsdrucksachen 17/14714 und 18/2257)?

Die vom Haushaltsausschuss des Deutschen Bundestages bewilligten 30 Stellen für das Kompetenzzentrum Informationstechnische Überwachung (CC ITÜ) sind derzeit bis auf zwei Stellen besetzt.

- a) In welcher Höhe war das CC ITÜ im Jahr 2014 mit Finanzmitteln ausgestattet, und wie ist der Haushaltansatz für das Jahr 2015?
- b) Wie verteilen sich die Finanzmittel vom Jahr 2014 auf die Beschaffung bzw. Programmierung von Überwachungssoftware nach Maßgabe der gesetzlichen Befugnisse, bei denen es sich nach Ansicht der Fragesteller um staatliche Trojaner handelt (Bundestagsdrucksache 18/2257) sowie andere Soft- und Hardware zur „informationstechnischen Überwachung“, und um welche Anwendungen handelt es sich dabei konkret?

Die Fragen 9a und 9b werden gemeinsam beantwortet.

In den Bundeshaushalten für die Jahre 2014 und 2015 erhielt bzw. erhält das Bundeskriminalamt eine bedarfsgerechte Veranschlagung der personellen und finanziellen Ressourcen, die es zur Erfüllung seiner gesetzlichen Aufgaben be-

nötigt. Die Ausgaben für das CC ITÜ als originärer Aufgabenbereich werden aus den vorhandenen Haushaltsansätzen getragen und nicht gesondert erfasst.

Die sich aus steigenden Anforderungen an die Qualität und Quantität der Aufgabenwahrnehmung möglicherweise ergebenden zusätzlichen Bedarfe an Haushaltsmitteln macht das Bundeskriminalamt regelmäßig in den regulären Verfahren der Haushaltsaufstellung geltend. Für das CC ITÜ wurden in den Haushalten 2014 und 2015 keine zusätzlichen Haushaltsmittel veranschlagt.

- c) Welche Akteure (Ämter, Behörden, Institute, Firmen, Stiftungen etc.) wurden im zweiten Halbjahr 2014 (auch zwischenzeitlich) in deren Entwicklung und Anwendung eingebunden, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Gegenüber der Darstellung auf den Bundestagsdrucksachen 17/14714 vom 6. September 2013 bzw. 18/2257 vom 1. August 2014 hat sich zwischenzeitlich folgende Änderung ergeben: Die Unterstützung durch das Land Hessen wurde beendet.

- d) Welche Firmen oder Institute haben in welchem Zusammenhang eine unterstützende und beratende Funktion wahrgenommen?

Es haben sich keine Änderungen gegenüber den Angaben zum ersten Halbjahr 2014 in der Antwort der Bundesregierung zu Frage 9d der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014 ergeben.

10. Wie oft haben welche Bundesbehörden im zweiten Halbjahr 2014 Trojanerprogramme eingesetzt?
- a) Welches der verfügbaren Programme (etwa „Übergangslösung“, Trojaner zur „Onlinedurchsuchung“, Trojaner zur „Quellen-TKÜ“) kam dabei jeweils zur Anwendung?
- b) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?
- c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
- d) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage teilweise nicht offen beantwortet werden kann. Die erbetene Antwort nach der Anzahl der durch den Bundesnachrichtendienst (BND) eingesetzten Überwachungssoftware ist geheimhaltungsbedürftig. Die Antwort enthält Informationen zur Arbeitsweise und zu der eingesetzten nachrichtendienstlichen Methodik des BND. Hier sind insbesondere die Aufklärungsaktivitäten des BND betroffen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des Bundesnachrichtendienstes stellt für die erfolgreiche Aufgabenerfüllung einen überragend wichtigen Grundsatz dar und dient der Aufrechterhaltung der Effektivität der Beschaffung von nachrichtendienstlich relevanten Informationen. Der Schutz der Aufklärungsfähigkeit des BND dient daher dem Staatswohl. Es steht zu befürchten, dass durch das Bekanntwerden der erfragten Informationen ein Nachteil für die Auftragserfüllung eintreten könnte.

Bereits die Information, ob bzw. in welchem Umfang der BND Überwachungssoftware einsetzt, kann zu einer wesentlichen Schwächung der Aufgabenerfüllung führen. Die Offenlegung dieser Informationen kann mithin die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Aus diesem Grund sind die Informationen als Verschluss-sache gemäß der VSA mit dem VS-Grad „VS – Geheim“ eingestuft.⁹

Die weitere Beantwortung der Frage betrifft solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufte Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls im Verfassungsrang stehende schutzwürdige Interessen wie das Staatswohl begrenzt. Mit einer substantiierten Beantwortung dieser Fragen würden Einzelheiten zur Methodik des BND benannt, die die weitere Arbeitsfähigkeit und Aufgabenerfüllung auf dem spezifischen Gebiet der technischen Aufklärung gefährden würden.

Eine Bekanntgabe von Einzelheiten zu nachrichtendienstlichen Verfahren zur Erhebung von Daten aus zugriffsgeschützten Bereichen von IT-Infrastrukturen im Ausland im Rahmen der technischen Aufklärung würde weitgehende Rückschlüsse auf die technischen Fähigkeiten und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential des BND zulassen. Dadurch könnte die Fähigkeit des BND, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des BND jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Derartige Erkenntnisse dienen insbesondere auch der Beurteilung der Sicherheitslage in den Einsatzgebieten der Bundeswehr im Ausland. Ohne dieses Material wäre eine solche Sicherheitsanalyse nur noch sehr eingeschränkt möglich, da das Sicherheitslagebild zu einem nicht unerheblichen Teil aufgrund von Informationen, die durch die technische Aufklärung gewonnen werden, erstellt wird. Das sonstige Informationsaufkommen des BND ist nicht ausreichend, um ein vollständiges Bild zu erhalten und Informationsdefizite im Bereich der technischen Aufklärung zu kompensieren.

Insofern birgt eine Offenlegung der erfragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen technischen Fähigkeiten des BND bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und technische Fähigkeiten des BND gewinnen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des BND – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Bundesnachrichtendienstgesetzes) – nicht mehr sachgerecht erfüllt werden könnte.

Eine VS-Einstufung und Hinterlegung der erfragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung des BND nicht ausreichend Rechnung tragen. Die erfragten Inhalte beschreiben die technischen Fähigkeiten des BND so detailliert, dass eine Be-

⁹ 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.

kanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Dies gilt umso mehr, als sie Spezifika betreffen, deren technische Umsetzung nur in einem bestimmten Verfahren erfolgen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente möglich.

Aus dem Vorgenannten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse des BND zurückstehen.

Im Übrigen wird auf den als „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.¹⁰

Durch die Bundeswehr, die Zollverwaltung, das BKA, die BPOL, das Bundesamt für Verfassungsschutz (BfV) und in Umsetzung von Beschlüssen des Ermittlungsrichters des Bundesgerichtshofes wurde im erfragten Zeitraum keine Überwachungssoftware im Sinne der Frage eingesetzt.

11. Welche Bundesbehörden sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone sogenannte Stille SMS zum Ausforschen des Standortes ihrer Besitzerinnen und Besitzer oder dem Erstellen von Bewegungsprofilen zu verschicken, bzw. welche Änderungen haben sich gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Gegenüber dem ersten Halbjahr 2014 (siehe Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014) haben sich – mit Ausnahme des als „VS – Geheim“ eingestuften Antwortteils gemäß der Vorbemerkung der Bundesregierung, auf den insoweit verwiesen wird – keine Änderungen ergeben.¹⁰

- a) Wie viele „Stille SMS“ wurden von den jeweiligen Behörden im zweiten Halbjahr 2014 jeweils versandt (bitte bezüglich des Zollkriminalamtes nach den einzelnen Zollfahndungsämtern aufschlüsseln)?

Jahr	BfV	BKA	BPOL	MAD	Zoll
2. Halbjahr 2014	142 108	26 915	39 409	0	(*)

(*) Für den Bereich des Zollfahndungsdienstes wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.¹¹

- b) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung differenzieren)?

Für das BKA, die BPOL und den GBA ist eine Aufschlüsselung im Sinne der Frage nicht möglich.

Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.¹¹

¹⁰ 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 Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

- c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?

Der Bundesregierung liegen dazu keine statistischen Informationen vor. Auf die Antwort zu Frage 11b wird verwiesen.

Ergänzend wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.¹²

- d) Welche Hard- und Software wird hierfür genutzt, und welche Änderungen haben sich hierzu gegenüber dem ersten Halbjahr 2014 ergeben (Bundestagsdrucksache 18/2257)?

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 10 auf Bundestagsdrucksache 18/2257 vom 1. August 2014 und im Übrigen auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.¹²

- e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

In der Praxis der Strafverfolgungsbehörden erfolgt die Erhebung der Daten nach dem Versenden einer „Stillen SMS“ im Rahmen von Telekommunikationsüberwachungsmaßnahmen nach den §§ 100a, 100b StPO. Diese dürfen nur angeordnet werden, wenn der Verdacht des Vorliegens einer schweren Straftat im Sinne des § 100a Absatz 2 StPO, die auch im Einzelfall schwer wiegt, besteht und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der betroffenen Personen auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Ermittlung der Aufenthaltsorte der Täter oder Teilnehmer einer schweren Straftat im Sinne des § 100a Absatz 2 StPO wird in diesen Fällen grundsätzlich als wesentlich eingeschätzt.

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

Es wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. zu Frage 13 auf Bundestagsdrucksache 18/2257 vom 1. August 2014 verwiesen.

¹² Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

