Deutscher Bundestag **Drucksache 18/2932**

18. Wahlperiode 17.10.2014

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/2613 –

Neue digitale Überwachungsmethoden

Vorbemerkung der Fragesteller

Die Polizeien und Geheimdienste des Bundes verfügen über technische Werkzeuge (Hardware, Software) zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten (Bundestagsdrucksache 17/12651). Hersteller und Funktionalität der Produkte sind vielfach unbekannt. Mitgeteilt wird häufig lediglich, es würden „handelsübliche wie auch eigenentwickelte Hard- und Software“ genutzt. Auch für neuere Internetdienste (etwa Cloud-Verfahren) werden Verfahren zum Abhören von Metadaten oder Mitlesen von Inhalten entwickelt (Plenarprotokoll 17/210). Die rechtliche Grundlage ist dabei vielfach unklar und bezieht sich auf Gesetze, die lange vor der Einführung der neuen Dienste erlassen wurden. Dies gilt ebenso für neuere, digitale Ortungsverfahren, wie etwa von Mobiltelefonen. Im Bundesministerium des Innern (BMI) existieren deshalb immer wieder Arbeitsgruppen, die rechtliche Rahmenbedingungen erörtern sollen. Die Rede ist von „organisatorischen und personellen Herausforderungen, die sich aus den Entwicklungen auf dem Gebiet der Telekommunikation für die Sicherheitsbehörden ergeben“ (Bundestagsdrucksache 18/2257). Im BMI ist hierzu ein „Runder Tisch zur Sicherstellung der Telekommunikationsüberwachung in der Zukunft“ eingerichtet worden.

Vorbemerkung der Bundesregierung

Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Fragen 1, 2, 3, 10, 13, 15, 16 und 18 aus Geheimhaltungsgründen ganz oder teilweise nicht oder nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden können.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 15. Oktober 2014 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt.

Die teilweise Einstufung der Antworten auf die Fragen 1, 2, 10, 15 und 16 als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – NUR FÜR DEN DIENSTGEBRAUCH“ ist aber im vorliegenden Fall erforderlich. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung – VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt würden. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Auch die Antwort zu Frage 18 kann teilweise nicht offen erfolgen. Informationen über die technischen Fähigkeiten der Nachrichtendienste zur Ortung von Mobiltelefonen bzw. zur Eingrenzung des Standorts von Mobiltelefonen sind besonders schutzbedürftig. Eine Antwort würde Einzelheiten zu Arbeitsweisen, Strategien und Methoden offenlegen. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Nachrichtendienste nachteilig sein und die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern (BMI) zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „GEHEIM“ eingestuft. Sie werden zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Die weitergehende Beantwortung der Frage 1 sowie die Beantwortung der Fragen 3 und 13 muss im Interesse der Wahrung des Staatswohls unterbleiben. Auch eine Beantwortung durch Hinterlegung bei der Geheimschutzstelle des Deutsches Bundestages kommt nicht in Betracht, da die fraglichen Informationen von solcher Bedeutung sind, dass auch ein geringfügiges Risiko des Bekanntwerdens nicht hingenommen werden kann. Die Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Auftragserfüllung besonders schutzbedürftig. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik des Bundesnachrichtendienstes (BND) und des Bundesamtes für Verfassungsschutz (BfV) und insbesondere deren Aufklärungsaktivitäten, Aufklärungsmöglichkeiten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des BND und des BfV im Bereich der Telekommunikationsaufklärung stellt für die Aufgabenerfüllung der Nachrichtendienste einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Eine Veröffentlichung von konkreten technischen Einzelheiten wie der eingesetzten Hard- und Software würde zu einer wesentlichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Infor-

mationsgewinnung führen und ggf. Fähigkeitslücken offenbaren. Dies hätte für die Auftragserfüllung der Nachrichtendienste erhebliche Nachteile zur Folge.

Eine Antwort zu Frage 13 würde Informationen offenlegen, die eindeutige Rückschlüsse auf die Leistung und die damit verbundene Taktik im Einsatz ermöglichen. Die in der Frage angesprochenen und vom Bundeskriminalamt (BKA) beauftragten Fahrzeuge werden bei der verdeckten Informationsbeschaffung im Rahmen von Observations- und Fahndungseinsätzen benutzt. Informationen über die Fahrzeugausstattung in fernmeldetechnischer Hinsicht stehen daher in engem Zusammenhang mit den Aufklärungsmöglichkeiten des BKA. Ein Bekanntwerden der Überwachungstechniken in den Fahrzeugen würde zu einer erheblichen Beeinträchtigung bei der Gewinnung verdeckter Aufklärungsergebnisse (gemäß den Befugnisnormen der Strafprozessordnung) führen, da sich das polizeiliche Gegenüber im Verhalten und Handeln auf diese technischen Möglichkeiten einstellen kann. Bei Tatverdächtigen, die sensibel gegenüber polizeilichen Überwachungsmaßnahmen sind, würde ein Bekanntwerden dieser technischen Möglichkeiten dazu führen, dass die verdeckte Informationsbeschaffung in Phänomenbereichen des internationalen Terrorismus und der schweren und organisierten Kriminalität nahezu unmöglich würde. Die Offenlegung entsprechender Informationen ist daher nicht möglich.

1. Über welche technischen Werkzeuge (Hardware, Software) verfügen welche Bundesbehörden zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten, bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 17/12651 ergeben?

Zur Überwindung von Gerätesperrcodes bei Kommunikationsgeräten (Mobilfunkgeräten) werden im BKA kommerziell verfügbare Softwarewerkzeuge eingesetzt. Diese werden jedoch ausschließlich bei Mobilfunkgeräten angewendet, die zuvor im Rahmen von Ermittlungsverfahren bei strafprozessualen Maßnahmen unter Beachtung der damit verbundenen einschlägigen Rechtsvorschriften sichergestellt wurden.

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.[1]

Hinsichtlich der Werkzeuge, die im Bundesamt für Sicherheit in der Informationstechnik (BSI) Verwendung finden, hat sich gegenüber der Antwort auf die Kleine Anfrage der Fraktion DIE LINKE. vom 8. März 2013 (Bundestagsdrucksache 17/12651) keine Änderung ergeben.

Die Behörden der Zollverwaltung verfügen über keine eigenen technischen Werkzeuge (Hardware, Software) zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten. Im Bereich IT-Kriminaltechnik werden bei der Auswertung von Kommunikationsgeräten (z. B. Smartphones), die zuvor im Rahmen von Ermittlungsverfahren sichergestellt wurden, technische Werkzeuge zur Ermittlung von Passwörtern und der Überwindung von Gerätesperren eingesetzt.

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

Im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) verfügt keine Behörde über spezifische technische Werkzeuge zum Auslesen, Erraten oder Knacken von Passwörtern. Im Rahmen einer Telekommunikationsüberwachung ist es dem Militärische Abschirmdienst (MAD) möglich, übermittelte

[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.

Passwörter mitzulesen. Im Übrigen wird auf die Antwort zu Frage 25 auf Bundestagsdrucksache 17/12651 verwiesen.

2. Welche „kommerziell verfügbare[n] Softwarewerkzeuge“ werden hierfür im Bundeskriminalamt (BKA) eingesetzt?

Auf die Antwort zu Frage 1 wird verwiesen.

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.[2]

3. Welche „handelsübliche wie auch eigenentwickelte Hard- und Software“ wird vom Bundesnachrichtendienst (BND) und vom Bundesamt für Verfassungsschutz (BfV) „zur Entzifferung“ eingesetzt (bitte die Hersteller sowie die weiteren Beteiligten der „Eigenentwicklungen“ benennen)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

4. Inwiefern hält die Bundesregierung Möglichkeiten für Behörden des BMI zum Knacken oder Umgehen von Verschlüsselung für unabdingbar oder entbehrlich?

Die Notwendigkeit zum „Knacken oder Umgehen“ von Verschlüsselungen im Internet hängt vom jeweiligen Einzelsachverhalt und dem Vorliegen der rechtlichen Voraussetzungen ab. Im Rahmen ihrer Aufgabenerfüllung wie etwa der Strafverfolgung sind im Einzelfall entsprechende Maßnahmen der Behörden im Geschäftsbereich des BMI unter Wahrung der gesetzlichen Voraussetzungen zu treffen.

5. In wie vielen Fällen war eine Verschlüsselung nach Einschätzung der Bundesregierung hinderlich bei der Ermittlung, bzw. in wie vielen Fällen hat eine nachträgliche Entschlüsselung wesentlich zur Aufklärung von Tatkomplexen beigetragen?

Der Anteil digitaler Speichermedien an beschlagnahmten oder sichergestellten Beweismitteln nimmt aufgrund der weiten Verbreitung der Digitaltechnik im täglichen Leben kontinuierlich zu. Die beschlagnahmten oder sichergestellten Beweismittel sind potentiell immer für die Ermittlungen von Bedeutung. Durch die technischen Möglichkeiten der Sicherung (z. B. mittels PIN oder Passwort) wird die Auswertung der Beweismittel zunehmend verhindert oder erschwert.

Das BKA führte im Zeitraum vom 1. Januar 2012 bis zum 31. Dezember 2013 im Auftrag des AK II eine Erhebung unter Ermittlungsverfahren im Bereich der schweren Kriminalität (§ 100a Absatz 2 der Strafprozessordnung – StPO) durch, bei denen Ermittlungsdefizite aufgrund des Einsatzes verschlüsselter Kommunikation bestanden.

In 97 Prozent der betrachteten 292 Fälle wurden Instant-Messaging-Dienste mit zumeist integrierter Verschlüsselung verwendet, in über 70 Prozent der Fälle konnte die Nutzung von Kryptierung belegt werden. Bei allen der betrachteten Verfahren im Bereich der schweren Kriminalität (§ 100a Absatz 2 StPO) bestan-

[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.

den Ermittlungsdefizite, weil die Überwachung oder Auswertung verschlüsselter Kommunikation nicht möglich war. Eine Statistik im Sinne der Anfrage wird durch BKA, Bundespolizei und Zollverwaltung nicht geführt.

6. Inwiefern trifft es zu, dass der BND in Afghanistan, Somalia und/oder dem Nahen Osten „jegliche Art von Kommunikation“ abhört und speichert und hiermit „Telefonie, Internetnutzung, E-Mail, GPS-Datenverarbeitung etc.“ gemeint ist (DER SPIEGEL, 8. September 2014)?

Zur Gewinnung auftragskonformer Erkenntnisse von außen- und sicherheitspolitischer Relevanz (vgl. § 1 Absatz 2 des Bundesnachrichtendienstgesetzes – BNDG) setzt der BND im Rahmen der gesetzlichen Vorgaben auch das Mittel der Fernmeldeaufklärung ein. Eine anlasslose Vollerfassung sämtlicher Telekommunikationsverkehre findet nicht statt.

7. Welche weiteren Länder wurden auf diese Weise in den Jahren 2013 und 2014 von der ehemaligen Echelon-Station Bad Aibling in Bayern abgehört?

Die Dienststelle des BND in Bad Aibling war zu keiner Zeit Teil eines Verbundes mit der Bezeichnung „Echelon“. Ergänzend wird auf die Antwort zu Frage 6 verwiesen.

8. Inwiefern hat die Bundesregierung gegenüber den USA versucht zu klären, ob Berichte zutreffen, wonach sich der Militärgeheimdienst NSA Zugriff auf deutsche Internetnetzwerke verschafft hat, wozu laut einem Dokument des Whistleblowers Edward Snowden die Telekom Deutschland GmbH und der Kölner Provider NetCologne Gesellschaft für Telekommunikation mbH gehören (SPIEGEL ONLINE, 17. September 2014)?

Nachrichtendienstliche Fragen nimmt die Bundesregierung mit der amerikanischen Regierung im Rahmen des strukturierten Dialogs auf.

a) Sollten diese Berichte zutreffen, welcher Straftat hätten sich die USA in diesem Falle schuldig gemacht?

Es wird auf die Antwort zu Frage 90 auf die Kleine Anfrage der Fraktion der SPD „Abhörprogramme der USA und Umfang der Kooperation der deutschen Nachrichtendienste mit den US-Nachrichtendiensten“ auf Bundestagsdrucksache 17/14560 vom 14. August 2013 verwiesen.

b) Sofern die Bundesregierung hierzu gegenüber den USA nicht tätig wurde, auf welche Weise wird sie diesem Verdacht einer möglichen Straftat nachgehen?

Dem vom Nachrichtenmagazin „DER SPIEGEL“ in der Ausgabe 38/2014 geäußerten Verdacht, die National Security Agency (NSA) habe sich Zugriff auf das Netzwerk der Deutschen Telekom und des Anbieters Netcologne verschafft, wird beim Generalbundesanwalt beim Bundesgerichtshof (GBA) in einem Beobachtungsvorgang nachgegangen. Auch das BSI ist derzeit zusammen mit weiteren Behörden im Rahmen der Analyse des Sachverhalts aktiv. Weitere Auskünfte werden erst nach Abschluss der Analyse möglich sein.

9. Welche neueren Details kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung sowie einer „Verschlüsselung im Bereich des Cloud-Computing im Allgemeinen“ beschäftigt (Plenarprotokoll 17/210)?

Das Projekt CLOUD wurde im Strategie- und Forschungszentrum Telekommunikation (SFZ TK) auf Basis des Auftragnehmerberichts von März 2013 abgeschlossen. Gegenüber den Auskünften auf Bundestagsdrucksache 17/12651 gibt es keine neuen Details.

a) Welche „fachliche[n] Fragestellungen“ wurden vom BKA, der Bundespolizei oder dem BfV im Rahmen des Projekts „CLOUD“ formuliert (Bundestagsdrucksache 17/12651)?

Die Fragestellungen befassten sich mit begrifflichen, technischen und juristischen Aspekten im Bereich Cloud Computing und deren Auswirkung auf die Telekommunikationsüberwachung (TKÜ) der Sicherheitsbehörden.

Gegenstand des Projekts war unter anderem die Abgrenzung von Cloud- und Webdiensten, die in Cloud Computing angewendeten Technologien und die rechtlichen Auswirkungen der Internationalisierung auf die technische Diensteerbringung.

b) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen erbringen welche Leistungen für das Projekt?

Das Projekt ist abgeschlossen, es werden keine weiteren Leistungen erbracht. Auf die Antwort zu Frage 9 wird verwiesen.

10. Welche wesentlichen (Zwischen-)Ergebnisse kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, und welche Schlussfolgerungen zieht sie daraus?

Die Überwachung von Cloud-Diensten im Rahmen von TKÜ-Maßnahmen wird durch Einsatz von Verschlüsselungstechnologien erschwert. Aus Sicht der Bundesregierung ist es erforderlich, die weitere Entwicklung von Cloud Computing zu verfolgen.

a) Welche „potentiellen technischen Möglichkeiten für einen Zugriff der Sicherheitsbehörden“ wurden identifiziert?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.[3]

b) Welche „rechtlichen Rahmenbedingungen“ wurden erörtert?

Es wurden die rechtlichen Rahmenbedingungen erörtert, die sich aus der Internationalisierung der technischen Diensteerbringung 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.

c) Inwiefern hält die Bundesregierung technische Möglichkeiten zum Knacken der Passwörter von Cloud-Diensten zur Strafverfolgung als von der Strafprozessordnung gedeckt?

§ 100j StPO regelt den Zugriff auf Daten, mittels derer der Zugriff auf Speichereinrichtungen, die räumlich getrennt von Endgeräten eingesetzt werden, geschützt wird. § 110 Absatz 3 StPO sieht vor, dass die Durchsicht eines elektronischen Speichermediums bei dem von einer Durchsuchung Betroffenen auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden darf, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist.

11. Von welchen Möglichkeiten zur Überwachung bzw. der Rekonstruktion der Nutzung von digitalen Kopiergeräten haben Bundesbehörden bereits Gebrauch gemacht?

Im Rahmen der Erhebung des kriminaltechnischen Sachbeweises zur Unterstützung von polizeilichen Ermittlungen kann das Kriminaltechnische Institut des BKA die in den Farbkopien enthaltene Signatur feststellen (ID-Dekodierung bei elektrofotografischen Geräten). Diese Signatur kann an Europol übermittelt werden, welche über eine Anfrage bei den Geräteherstellern das jeweilige Kopiergerät (und ggf. den Standort) identifizieren kann.

a) Was ist der Bundesregierung darüber bekannt, inwiefern digitale Kopierer über technische Möglichkeiten zum automatisierten Aufspüren kopierter Banknoten oder andere Wertpapiere verfügen?

Den Behörden der Bundesverwaltung ist bekannt, dass es technische Möglichkeiten zum automatisierten Aufspüren kopierter Banknoten oder Wertpapiere gibt. Die Hersteller rüsten Kopierer in der Regel mit einem Banknotenerkennungssystem aus. Die Banknoten werden beim farbigen Scannen als solche erkannt und je nach Typ erfolgt entweder eine Fehlermeldung, ein Schwarzdruck oder ein dunkler Graudruck.

Darüber hinaus gibt es geräteabhängig Kennzeichnungen. So ist etwa der sogenannte MIC (Machine Identification Code), auch Farbdruckermarkierung oder Tracking Dots genannt, bekannt. Dabei handelt es sich meist um auf der Kopie für den Nutzer nicht sichtbar angeordnete gelbe Punkte. Aus diesen Punkten können durch den Hersteller ggf. Angaben über die Seriennummer des Druckers sowie Datum und Uhrzeit des Drucks ausgelesen werden. Dies ermöglicht die Identifizierung des Drucksystems und damit eine Rückverfolgung.

b) Inwiefern und nach welchem Verfahren werden welche Bundesbehörden von Herstellern oder Aufstellern von Stand-alone-Kopierern oder netzangebundenen Kopierern benachrichtigt, wenn mit diesen Banknoten oder andere Wertpapiere vervielfältigt werden?

Der Bundesregierung ist eine entsprechende Benachrichtigung nicht bekannt.

c) Welche Bundesbehörden nutzen für polizeiliche oder geheimdienstliche Zwecke in Kopien verborgene Kennzeichen der Kopierer, und um welche technischen Verfahren handelt es sich dabei?

Verfahren, mit dem in bestimmten Fällen die Zuordnung von Farbkopierprodukten zu dem jeweiligen Ausgabegerät möglich ist, werden vom BKA und der Bundespolizei genutzt. Im Übrigen wird auf die Antwort zu Frage 11 verwiesen.

12. Worum handelt es sich bei den an die Firma ELETTRONICA GmbH vergebenen Aufträge „Ausbau von drei kriminalpolizeilichen Spezialfahrzeugen für das Bundeskriminalamt“ sowie „Ausbau von zwei Fahrzeugen für die Bundespolizei“ (Bundestagsdrucksache 18/2292)?

Seit Ende 2013 bestanden im Zusammenhang mit Ausbauten von Kriminalpolizeilichen Spezial-, Einsatz- und Unterstützungsfahrzeugen (KP-SEUF) für das BKA insgesamt drei Firmenkontakte zu der Firma ELETTRONICA. Alle drei Kontakte (zwei abgeschlossene Ausbauten und ein aktueller Ausbau) erfolgten nach der jeweils gültigen Leistungsbeschreibung für MEK-Fahrzeuge des Beschaffungsamtes des BMI.

Die Fahrzeuge der Bundespolizei werden im Flugdienst als mobile Führungsstellen verwendet und dienen der Kommunikation mit Polizeihubschraubern.

13. Welche Überwachungstechnik welcher Firmen ist in den Fahrzeugen verbaut?

Für das BKA wird auf die Vorbemerkung der Bundesregierung verwiesen. In den in der Antwort zu Frage 12 genannten Fahrzeugen der Bundespolizei ist keine Überwachungstechnik verbaut.

14. Worum handelte es sich bei der Lieferung einer „Nachbearbeitungsplattform Strix“ für das BKA durch die Firmen MEDAV GmbH und/oder Vidit Systems GmbH (Bundestagsdrucksache 18/2292)?

Die „Nachbearbeitungsplattform Strix“ ist das Ergebnis des von der MEDAV GmbH durchgeführten „Forschungsprojekts zur prototypischen Realisierung einer Verarbeitungsplattform für Daten aus Telekommunikationsüberwachungen“ (vgl. Bundestagsdrucksache 18/2292 vom 6. August 2014).

15. Welche Fragestellungen bzw. technischen Lösungen hat das „Forschungsprojekt zur prototypischen Realisierung einer Verarbeitungsplattform für Daten aus Telekommunikationsüberwachungen“ mit der Firma MEDAV GmbH untersucht (Bundestagsdrucksache 18/2292)?

Es war zu betrachten, inwieweit einzelne Werkzeuge zur Untersuchung und Dekodierung von TKÜ-Daten automatisiert eingesetzt werden können. Die Grenzen und Möglichkeiten dafür sollten im Rahmen einer prototypischen Realisierung einer Nachbereitungsplattform aufgezeigt werden.

a) Welche weiteren Partner erhielten welche weiteren Aufträge?

Der Auftrag zur Nachbereitungsplattform STRIX wurde nur an die MEDAV GmbH vergeben.

b) Welche Ergebnisse zeitigte das Projekt, und welche Schlussfolgerungen zieht die Bundesregierung daraus?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.[4]

16. Welche Studien oder Projekte zur Überwachung (nicht Ortung) von Smartphones haben Behörden des BMI, des Bundesministeriums der Verteidigung oder des Bundeskanzleramtes in den vergangenen fünf Jahren durchgeführt bzw. deren Ergebnisse angefordert (um einen Überblick über etwaige grundrechtsrelevante Verfahren zu bekommen, bitte die Zielsetzung der Studien oder Projekte kurz schildern), und wer sind die Auftragnehmer oder Unterauftragnehmer jener Studien oder Projekte?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.[4]

Der Geschäftsbereich des BMVg führt das Projekt „System zur Aufklärung zellularer Netze, 2. Generation (AZN)“ durch. Dieses System dient der signalerfassenden Aufklärung von zellularen Mobilfunkverkehren in den Einsatzgebieten der Bundeswehr und soll einen Beitrag zur militärischen Nachrichtenlage zu liefern.

Das System verfügt über einen Filtermechanismus, der eine automatische Filterung von G10-Metadaten oder auch eine durch autorisierte Nutzer gesteuerte manuelle Filterung unter Anlage einer umfassenden Historie bzw. eines umfassenden Protokolls durchführt. Für weitere Einzelheiten wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.[4]

17. Welche Fragestellungen bzw. technischen Lösungen hat das Forschungsprojekt „Mehrwegepeiler und Systemdemonstrator“ der Firma MEDAV GmbH im Rahmen des Verbundvorhabens „Emitter Identifikation und Lokalisierung unter Mehrwegeausbreitungsbedingungen“ (EILT) untersucht (Bundestagsdrucksache 18/2292)?

Ziel des Verbundprojektes war die Lokalisierung nicht kooperierender Funkemitter unter komplizierten Umgebungsbedingungen. Im Teilvorhaben „Mehrwegepeiler und Systemdemonstrator“ der Firma MEDAV GmbH wurden Einsatzszenarien definiert, ein Prototyp des Mehrwellenpeilers aufgebaut und validiert und die Arbeiten im Verbund koordiniert.

a) Welche technischen Verfahren zur Ausbreitung von Funksignalen bzw. deren Präzisions-Lokalisierungen wurden dabei genau untersucht?

Es werden reale Messungen mit Prädiktions- und Schätzverfahren kombiniert. Reale Messungen liefern Schätzergebnisse zu verschiedenen Ausbreitungswegen. Prädiktionsverfahren liefern Vorhersagen für Standorte des Senders, die zur gemessenen Situation führen können. Die Daten aus Messung und Prädiktion werden über Fusionsalgorithmen zusammengeführt, um die Lokalisierung von Funkemittern zu verbessern.

[4] 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.

b) Welche weiteren Partner erhielten welche weiteren Aufträge?

Das Projekt EILT wird nicht im Rahmen eines Auftrages, sondern als Verbundvorhaben durch Zuwendungen gefördert. Die weiteren Partner des Verbundes neben der MEDAV GmbH sind das Fraunhofer-Institut FKIE, die AWE Communications GmbH und die TU Ilmenau.

c) Welche Ergebnisse zeitigte das Projekt, und welche Schlussfolgerungen zieht die Bundesregierung daraus?

Die Laufzeit des Projekts EILT endete am 30. Juni 2014. Der Ergebnisbericht des Vorhabens ist dem Zuwendungsgeber Bundesministerium für Bildung und Forschung bis zum 31. Dezember 2014 vorzulegen. Die vorliegenden Zwischenberichte lassen erwarten, dass das erwartete Ziel des Vorhabens auch erreicht wurde.

18. Welche weiteren technischen Möglichkeiten oder Protokolle (außer IMSI-Catchern) werden von welchen Bundesbehörden zur Ortung von Mobiltelefonen bzw. einer Eingrenzung von deren Standort angewandt?

Die Bundespolizei nutzt Möglichkeiten zur Versendung von „Stillen SMS“ (auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/2257 vom 1. August 2014 und auf Bundestagsdrucksache 18/2695 vom 30. September 2014 wird verwiesen).

Das BKA hat zur Ortung von Mobiltelefonen mittels „MSC-Ortung“ einen Nutzungszugang auf einer Anlage des Landesamtes für Zentrale Polizeiliche Dienste (LZPD) der Polizei Nordrhein-Westfalen. Darüber hinaus kann im Rahmen einer aktiven TKÜ-Maßnahme der Standort eines überwachten Mobiltelefons mittels einer sogenannten Stillen SMS festgestellt werden. Es wird zudem darauf hingewiesen, dass im Wege einer „Stillen SMS“ entgegen dem langläufigen Sprachgebrauch nicht der Standort des Mobiltelefons, sondern der Standort der Mobilfunk-Basisstation, welche die gegenwärtig versorgende Funkzelle aufspannt und das betreffende Endgerät vermittlungstechnisch versorgt, ermittelt wird. Es kann sich somit eine reale Abweichung von wenigen Metern (Innenstädte der Ballungszentren) bis zu mehreren Kilometern (ländliche Bereiche) ergeben.

Das BfV verfügt über ein System eines externen Herstellers zum Versand von „Stillen SMS“ und zur Durchführung von MSC-Ortungen. Im Rahmen von TKÜ-Maßnahmen werden außerdem die Geokoordinaten der Basisstation des überwachten Mobilfunkanschlusses übertragen.

Beim BND erfolgt eine Eingrenzung des Standortes von Mobilfunktelefonen ohne die Möglichkeit einer Verifizierung und ohne Echtzeitfähigkeit mit Hilfe eines kommerziellen Dienstleisters. Der BND nutzt darüber hinaus, wenn technisch zugänglich und auftragsrelevant, Informationen zur Eingrenzung des Standorts von ausländischen Mobilfunktelefonen, die mit Methoden der Fernmeldeaufklärung im Ausland erhoben werden.

Es wird auf den als „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.[5]

[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.

Die Behörden der Zollverwaltung nutzen für die Standortbestimmung von Mobiltelefonen den Versand von Ortungsimpulsen („Stille SMS“) sowie die Möglichkeit der MSC-Ortung. Hierbei wird auf die technische Infrastruktur anderer Behörden zurückgegriffen. Eigene technische Systeme zur Ortung von Mobiltelefonen werden von den Behörden der Zollverwaltung nicht vorgehalten.

19. Inwiefern haben sich die Bundesbehörden des Innern, der Verteidigung oder das Bundeskanzleramt bereits mit dem Aufbau eigener Fähigkeiten zur Ortung von Mobiltelefonen durch das „Signalling System #7“ (Signalisierungssystem Nummer 7; SS7) befasst (Netzpolitik, 26. August 2014)?

    a) Welche Behörden, Institute oder Firmen haben hierfür welche Aufträge erhalten, und welche Verfahren wurden untersucht?

    b) Welche Bundesbehörden verfügen zu welchem Zweck über wie viele SS7-Zugänge?

    c) Inwiefern haben sich die Bundesbehörden des Innern, der Verteidigung oder das Bundeskanzleramt bereits mit der Abwehr oder Verhinderung einer Ortung von Mobiltelefonen durch das SS7 befasst?

    d) Welche Behörden, Institute oder Firmen haben hierfür welche Aufträge erhalten, und welche Verfahren wurden untersucht?

Die genannten Behörden haben sich nicht mit dem Aufbau eigener Fähigkeiten zur Ortung von Mobiltelefonen durch das „Signalling System #7“ befasst.

20. Welche Geschäftsbeziehungen unterhielt oder unterhält das BMI mit der Schweizer Firma N., die nach Medienberichten IMSI-Catcher (IMSI: International Mobile Subscriber Identity) unter anderem an ein „Todesschwadron aus Bangladesch“ verkauft haben soll (WOZ Die Wochenzeitung vom 4. September 2014)?

Das BMI unterhielt oder unterhält keine Geschäftsbeziehungen zur Schweizer Firma Neosoft.

21. Inwiefern wurde inzwischen mit dem Vorhaben „Wissenserschließung aus offenen Quellen“ (WeroQ) begonnen, bzw. aus welchem Grund ist ein Zuwendungsbescheid durch das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr an das Fraunhofer-Institut immer noch nicht erfolgt (Schreiben des BMI an den Abgeordneten Andrej Hunko vom 22. Juli 2014)?

Das Vorhaben „Wissenserschließung aus offenen Quellen“ wurde noch nicht begonnen, weil das Thema derzeit einer ministeriellen Prüfung im BMVg unterliegt. Nach Abschluss dieser Prüfung wird das BMVg über den Zuwendungsbescheid entscheiden.

    a) Welche „Textmining-Technologien“ sollen konkret untersucht werden?

Das Vorhaben hat zum Gegenstand, auf dem Markt verfügbare Textmining-Technologien zu identifizieren, zu vergleichen und bezüglich ihrer Eignung zur Erschließung und Auswertung textbasierter Daten zu bewerten, um so eine Empfehlung für die Bundeswehr aussprechen zu können.

b) Welche Schlussfolgerungen zieht die Bundesregierung aus einer Darstellung der Universität Rostock, die dem Schreiben des BMI vom 22. Juli 2014 hinsichtlich einer Kooperation mit dem Institut für grafische Wissensorganisation (Grawis) widerspricht (taz.die tageszeitung vom 15. August 2014)?

In der genannten Presseberichterstattung geht es unter anderem um die Frage der organisatorischen/institutionellen Anbindung von GRAWIS. Die Bundesregierung zieht hieraus keine Schlussfolgerungen.

c) Welche gemeinsamen Förderanträge der Universität Rostock mit dem Grawis sind der Bundesregierung bekannt?

Der Bundesregierung liegen keine Erkenntnisse vor.

22. Auf welche Art und Weise soll die „Echtzeitanalyse von Streaming-Daten“ durch den BND Informationsströme durchsuchen und dabei „Muster“ erkennen (Schreiben des BMI an den Abgeordneten Andrej Hunko vom 22. Juli 2014)?

a) Mithilfe welcher statistischer Verfahren sollen aus diesen Mustern „Tendenzen, Trends und Auffälligkeiten erkannt werden“?

Die Fragen 22 und 22a werden gemeinsam beantwortet.

In der „Echtzeitanalyse von Streaming-Daten“ sollen verschiedene Methoden der Datenanalyse unter Nutzung statistischer Verfahren zur Anwendung kommen. Die konkret zur Anwendung kommenden Algorithmen, denen eine Kombination unterschiedlicher statistischer Verfahren zu Grunde liegen wird, sind noch nicht entwickelt. Sie sollen im Rahmen einer Machbarkeitsuntersuchung auf ihre generelle Tauglichkeit und Robustheit geprüft werden.

b) Welche „Betreiber“ bieten nach Kenntnis der Bundesregierung welche „derartige[n] Daten (teilweise auch gegen Gebühr)“ zur Nutzung an?

Viele Social-Media-Anbieter („Betreiber“) bieten Schnittstellen für fremde Applikationen an. Diesbezüglich wird auf offen im Internet verfügbare Informationen verwiesen, zu denen beispielhaft folgende Webseiten zählen:

www.memonews.com/technologie/top-5-fakten-uber-social-media-apis-fur-social-media-monitoring,
www.gnip.com,
www.sysomos.com/solutions/api-data-partners,
www.programmableweb.com/category/social-apis.

23. Inwiefern trifft es, wie den Fragestellern bekannt ist, zu, dass das BKA eine Lizenz für die Software „IBM Content Analytics“ zur Vorhersage bzw. Erstellung von Prognosen zukünftiger Straftaten beschafft?

Das BKA hat eine Lizenz für die Software „IBM Content Analytics“ beschafft, allerdings nicht zur Vorhersage bzw. Erstellung von Prognosen zukünftiger Straftaten (auf die Antwort zu Frage 23c wird verwiesen).

a) Aus welchem Grund wurde das Projekt nicht auf Bundestagsdrucksache 18/707 (Frage 1) vom März 2014 beauskunftet?

Weder besaß das BKA zum damaligen Zeitpunkt eine Lizenz der oben genannten Software noch gab es zu dem genannten Zeitpunkt diesbezüglich ein entsprechendes Projekt.

b) Welche Laufzeit hat ein entsprechendes Forschungsprojekt, und wie wurde es ausgeschrieben?

Das Projekt hat eine Laufzeit vom 1. September 2014 bis zum 31. August 2015. Das Forschungsprojekt wurde über das Beschaffungsamt des BMI im Rahmen eines Verhandlungsverfahrens ohne vorherige öffentliche Vergabebekanntmachung beschafft.

c) Welche Details kann die Bundesregierung zum Zweck eines entsprechenden Forschungsprojektes mitteilen, und welche Kosten entstehen hierfür?

Die Lizenz wurde beschafft, um große Datenmengen, welche ausschließlich im Rahmen von Ermittlungsverfahren sichergestellt wurden, zu analysieren bzw. auszuwerten. Bei dem Projekt soll festgestellt werden, inwieweit „IBM Content Analytics“ als kommerzielles Produkt in der Lage ist, die Auswertung dieser Daten im Rahmen von Ermittlungsverfahren zu unterstützen bzw. zu beschleunigen. Die entstehenden Kosten beziffern sich derzeit auf 515 000 Euro.

d) Welche weiteren Teilnehmenden (auch im Unterauftrag) sind der Bundesregierung hierzu bekannt, und worin genau besteht deren jeweiliger Auftrag?

Dem BKA sind keine weiteren Teilnehmenden bekannt.

e) Wo und auf welche Weise wird die Software getestet?

Die Software wird ausschließlich in den Räumlichkeiten des BKA, zunächst mit Testdaten, getestet. Die durch die Software erzielten Auswertungsergebnisse werden danach im Rahmen einer Evaluation mit den Ergebnissen der Auswertung durch die Sachbearbeiter verglichen.

f) Inwiefern wird die Software auch in konkreten Ermittlungsverfahren ausprobiert?

Die Software wurde noch nicht im Rahmen konkreter Ermittlungsverfahren eingesetzt. Derzeit wird nur mit Testdaten gearbeitet.

24. Mit welchen weiteren Herstellern sowie Landespolizeibehörden hatten Behörden des BMI hinsichtlich der Nutzung von Anwendungen zum „Predictive Policing“ Kontakt?

Das BKA hatte Kontakt zu den Kriminalistisch Kriminologischen Forschungsstellen des Landeskriminalamtes in Nordrhein-Westfalen sowie des Bayerischen Landeskriminalamtes. Ziel war die Identifikation von Ansprechpartnern sowie eine erste Information zu den dortigen Planungen im Zusammenhang mit predictive policing.

25. Welche aktuellen Marktsichtungen wurden hierzu mit welchem Ergebnis durchgeführt?

Eine Marktsichtung erfolgte nicht, lediglich eine Recherche in öffentlich zugänglichen Quellen bezogen auf kriminologische Aspekte wurde durchgeführt.

26. Welche „organisatorischen und personellen Herausforderungen, die sich aus den Entwicklungen auf dem Gebiet der Telekommunikation für die Sicherheitsbehörden ergeben“ wurden beim auf Bundestagsdrucksache 18/2257 beauskunfteten Treffen des „Runden Tischs zur Sicherstellung der Telekommunikationsüberwachung in der Zukunft des Bundesministeriums des Innern“ konkret besprochen?

Bei dem auf Bundestagsdrucksache 18/2257 beauskunfteten Treffen erfolgte keine inhaltliche Befassung. Das Treffen diente der Endredaktion des Arbeitsgruppenberichts.

27. Welche Maßnahmen hat das BMI daraufhin eingeleitet, bzw. welche weiteren Maßnahmen sind geplant?

Die Vorschläge der Arbeitsgruppen werden derzeit noch im BMI geprüft.

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