



Bundesministerium
des Innern, für Bau
und Heimat

POSTANSCHRIFT Bundesministerium des Innern, für Bau und Heimat, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117

FAX +49 (0)30 18 681-11019

INTERNET www.bmi.bund.de

DATUM 5. Februar 2020

BETREFF **Kleine Anfrage des Abgeordneten Andrej Hunko u. a.
und der Fraktion DIE LINKE.
Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern,
Funkzellenabfragen im zweiten Halbjahr 2019
BT-Drucksache 19/16427**

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte Antwort.

Hinweis:

Teile der Antwort sind VS-GEHEIM und VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

Mit freundlichen Grüßen
in Vertretung

Klaus Vitt

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin

VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof

Bushaltestelle Berlin Hauptbahnhof

Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.

Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellen-abfragen im zweiten Halbjahr 2019

BT-Drucksache 19/16427

Vorbemerkung der Fragesteller:

Halbjährlich fragen die Abgeordneten der Linksfraktion beim Bundesinnenministerium, beim Bundesfinanzministerium und beim Bundeskanzleramt nach den Zahlen von Einsätzen digitaler Fahndungsmethoden (Bundestagsdrucksachen 19/7104, 19/3678, 19/505, 18/11041, 18/4130, 18/2257, 18/5645, 18/7285, 18/9366, 18/11041). Hintergrund ist die zunehmende Überwachung und Analyse digitaler Verkehre, die das Vertrauen in die Freiheit des Internet und der Telekommunikation untergraben. Aus Antworten aus früheren Anfragen geht hervor, dass dies vor allem den polizeilichen Bereich betrifft: Der Einsatz „Stiller SMS“, sogenannter „WLAN-Catcher“ und „IMSI-Catcher“ nimmt zu. Aus Sicht der Fragestellerinnen und Fragesteller sind diese Maßnahmen mitunter rechtlich gar nicht gestattet, etwa der Einsatz „Stiller SMS“. Denn Polizei und Geheimdienste dürfen nur passiv die Kommunikation von Telefonen abhören, die „Stillen SMS“ werden aber von den Behörden erst erzeugt. Während die Bundesregierung zwar Angaben zu „Stillen SMS“ des Bundeskriminalamts und der Bundespolizei macht, bleiben Zahlen für den Zoll seit 2012 als Verschlusssache eingestuft. Hinsichtlich des Bundesnachrichtendienstes unterbleibt jede Mitteilung. Mit Beantwortung der Drucksache 19/7847 ging das Bundesministerium des Innern dazu über, ab 2019 auch die Zahlen zu „Stillen SMS“ des Bundesamtes für Verfassungsschutz (BfV) als „VS –Geheim“ einzustufen. Diese seien besonders schutzbedürftig, da sich „durch die regelmäßige halbjährliche Beantwortung [...] Einzelinformationen zu einem umfassenden Lagebild verdichten können“. Die halbjährlichen Abfragen führten zu solche einer „Verdichtung“, auf diese Weise könnten Rückschlüsse auf die „technischen Fähigkeiten“ des Inlandsgeheimdienstes gezogen werden (vgl. Schreiben des Parlamentarischen Staatssekretärs Günter Krings an den MdB Andrej Hunko vom 11. März 2019).

Die Wissenschaftlichen Dienste des Bundestages betonen hingegen, dass derartige Beschränkungen dem verfassungsrechtlichen Verhältnismäßigkeitsgebot unterliegen (WD 3 - 3000 - 121/19).

Die Bundesregierung muss demnach mildere, gleich geeignete Mitteln suchen, anstatt die vorher offen mitgeteilten Informationen nunmehr als „VS –Geheim“ einzustufen. Auch die Verschlussachenanweisung (VSA) bestimmt in § 15 S. 3, dass ein geringerer Einstufungsgrad oder ein anderes, einer Geheimhaltung gleich geeignetes Mittel Vorrang haben muss. So ließen sich den Wissenschaftlichen Diensten zufolge Informationen dergestalt abstrahieren, dass auf geschützte Interessen des Staates keine wesentlichen Rückschlüsse mehr möglich sind. Im Ergebnis könnten dem Bundestag so z. B. abstrakte Informationen offen übermittelt werden, sowie zugleich in der Geheimschutzstelle des Bundestages konkretere aber eingestufte Informationen.

Vorbemerkung der Bundesregierung:

Die durch die Fragesteller referenzierte unterschiedliche Antworttiefe ist der Bundesregierung bekannt. Aus den unterschiedlichen gesetzlichen Aufgabenbereichen und Befugnissen der von dieser Kleinen Anfrage betroffenen Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes, einschließlich der Nachrichtendienste des Bundes, resultieren abgeleitet aus dem Staatswohl für die erfragten Informationen jedoch unterschiedlich hohe Schutzanforderungen, denen in Abwägung mit den verfassungsrechtlich garantierten Informationsrechten des Deutschen Bundestages und seiner Abgeordneten sachgerecht nur in unterschiedlicher Weise Rechnung getragen werden kann.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. 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 Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen der oben genannten Bundesbehörden eine Beantwortung sämtlicher Fragen im Rahmen dieser Kleinen Anfrage in offener Form ganz oder teilweise nicht erfolgen kann.

Im Einzelnen:

Die Antworten zu den Fragen 1e, 2b, 2c, 2h, 3b, 3c, 3e, 3f, 7 (mit Unterfragen) und 8 sind in Teilen als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Dienststellen des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb sind die Antworten zu den genannten Fragen gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (VS-Anweisung – VSA) in Teilen als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Die Antworten zu den Fragen 1 (mit Unterfragen), 2 (mit Unterfragen), 3 (mit Unterfragen) und 8 wurden durch den Bundesnachrichtendienst (BND), das Bundesamt für Verfassungsschutz (BfV) und den Militärischen Abschirmdienst (MAD) als „GEHEIM“ eingestuft.

Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der Nachrichtendienste des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten der Nachrichtendienste des Bundes stellt für deren Aufgabenerfüllung 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 Einzelheiten betreffend solche Fähigkeiten würde in zunehmendem Maße zur Ineffektivität der eingesetzten Mittel führen, da Personen im Zielspektrum der Maßnahmen sich auf die Vorgehensweisen und Fähigkeiten der Sicherheitsbehörden einstellen und entsprechend auf andere Kommunikationswege ausweichen könnten. Dies hätte - mit Blick auf das derzeitige Kommunikationsverhalten der im Fokus stehenden Akteure - eine wesentliche Schwächung der den Nachrichtendiensten des Bundes zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung zur Folge. Dies würde für die Auftragserfüllung von BND, BfV und MAD erhebliche Nachteile zur Folge haben. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen.

Deshalb sind die entsprechenden Informationen als Verschlussache gemäß § 2 Absatz 2 Nummer 2 der VSA „GEHEIM“ eingestuft und werden zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

Frage 1:

Wie oft haben welche Bundesbehörden im zweiten Halbjahr 2019 von „WLAN-Catchern“ Gebrauch gemacht?

- a) Welche Bundesbehörden haben zwar selbst keine „WLAN-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?*
- b) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?*
- c) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?*
- d) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?*
- e) Welche Hard- und Software wird für die „WLAN-Catcher“ genutzt bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben?*
- f) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?*

Zu 1:

Der Zoll und die Bundespolizei (BPOL) haben im zweiten Halbjahr 2019 keine WLAN-Catcher eingesetzt.

Beim Bundeskriminalamt (BKA) kam es in den in der Antwort zu Frage 1a genannten zwei Fällen des Generalbundesanwalts beim Bundesgerichtshof (GBA) zu einem solchen Einsatz.

Im Übrigen wird auf den als „GEHEIM“ eingestufteten Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 1a:

Das BKA, die BPOL und der Zoll haben sich keiner Amtshilfe für den Einsatz des „WLAN-Catchers“ bedient.

In zwei Ermittlungsverfahren des GBA wurde von WLAN-Catchern Gebrauch gemacht. Der Einsatz erfolgte durch das BKA.

Im Übrigen wird auf den als „GEHEIM“ eingestufteten Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 1b:

In den in der Antwort zu Frage 1a genannten Verfahren des GBA im Rahmen der Strafverfolgung war jeweils ein Beschuldigter betroffen.

Es wird auf den als „GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 1c:

In einem der der Antwort zu Frage 1a genannten Verfahren des GBA ist eine Benachrichtigung erfolgt.

Im anderen Ermittlungsverfahren steht die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegen.

Im Übrigen wird auf den als „GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 1d:

Es wird auf die Antwort der Bundesregierung zu Frage 1 und 1a auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/12465 vom 16. August 2019 verwiesen.

Zu 1e:

Es wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Soweit sich die Fragestellung auf die Nachrichtendienste des Bundes bezieht, ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Frage nicht beantwortet werden kann. Gegenstand der Frage sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Bekanntgabe von Einzelheiten zu der im Rahmen der erfragten Maßnahmen genutzten Hard- und Software würde weitgehende Rückschlüsse auf die technischen Fähigkeiten und unmittelbar auf die technische Ausstattung und das Aufklärungspotential der Nachrichtendienste des Bundes zulassen. Dadurch könnten die Fähigkeiten der Nachrichtendienste des Bundes, 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 der Nachrichtendienste des Bundes jedoch unerlässlich.

Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies betrifft insbesondere die Möglichkeiten zur Aufklärung nationaler und internationaler terroristischer Bestrebungen, bei denen derartige Kommunikationsmittel in besonderem Maße von den beobachteten Personen genutzt werden.

Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten der Nachrichtendienste des Bundes bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten der Nachrichtendienste des Bundes gewinnen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes (§ 1 Absatz 2 Gesetz über den Bundesnachrichtendienst [BNDG], § 3 Absatz 1 Bundesverfassungsschutzgesetz [BVerfSchG], § 1 Absatz 1 und § 14 Absatz 1 Gesetz über den militärischen Abschirmdienst [MADG]) nicht mehr sachgerecht erfüllt werden könnte.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Telekommunikationsüberwachung für die Aufgabenerfüllung der Nachrichtendienste des Bundes nicht ausreichend Rechnung tragen, weil insofern auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, mittels welcher technischen Mittel die Nachrichtendienste des Bundes von diesen Maßnahmen Gebrauch machen, könnte zu einer Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, die eine weitere Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Aus dem Vorgesagten 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 den Geheimhaltungsinteressen der Nachrichtendienste des Bundes zurückstehen.

Zu 1f:

Grundsätzlich dient die Maßnahme des Einsatzes des „WLAN-Catchers“ zur Erforschung des Sachverhaltes. Der Entscheidung des zuständigen Gerichts über die Anordnung dieser Maßnahme müssen Sachverhalte zu Straftaten von auch im Einzelfall erheblicher Bedeutung zugrunde liegen. Die Ermittlung der Umstände der Kommunikation der Täter oder Teilnehmer einer solchen Straftat sind daher grundsätzlich wesentlich.

In einem der in der Antwort zu Frage 1a genannten Verfahren des GBA konnten der Sachaufklärung dienende Erkenntnisse gewonnen werden.

Frage 2:

Welche Bundesbehörden haben im zweiten Halbjahr 2019 wie oft „IMSI-Catcher“ eingesetzt?

- a) Welche Bundesbehörden haben zwar selbst keine „IMSI-Catcher“ eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?
- b) Welche Hard- und Software wird für die „IMSI-Catcher“ genutzt?
- c) Wie viele Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?
- d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
- e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?
- f) Inwiefern haben die Maßnahmen im zweiten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?
- g) Für welche deutschen Firmen bzw. Lizenznehmer ausländischer Produkte wurden seitens der Bundesregierung im zweiten Halbjahr 2019 Ausfuhrgenehmigungen für sogenannte IMSI-Catcher in welche Bestimmungsländer erteilt?
- h) Wie viele IMSI-Catcher bzw. ähnliche Abhöranlagen für den Mobilfunkverkehr haben das Bundesamt für Sicherheit in der Informationstechnik oder andere zuständige Bundesbehörden (auch in deren Auftrag) im zweiten Halbjahr 2019 im Regierungsviertel oder in räumlicher Nähe anderer Bundesbehörden aufgespürt, und welche Betreiber der Anlagen wurden ausfindig gemacht?

Zu 2:

Im angefragten Zeitraum wurde das Einsatzmittel „IMSI-Catcher“ in 32 Fällen durch die BPOL und in 14 Fällen durch das BKA in bereits abgeschlossenen Gefahrenabwehrvorgängen oder Ermittlungsverfahren zum Einsatz gebracht.

Im Übrigen wird auf den als „GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 2a:

Im zweiten Halbjahr 2019 wurden in den Ermittlungsverfahren des GBA in 18 Fällen „IMSI-Catcher“ durch das BKA, die Landeskriminalämter Baden-Württemberg, Bayern und Niedersachsen, die Polizeipräsidien Nordhessen und Mönchengladbach sowie die Polizeiinspektion Halle eingesetzt.

Für die Einsätze des Zolls wurde im Rahmen der Amtshilfe auf die Geräte des BKA, der BPOL sowie verschiedener Landeskriminalämter zurückgegriffen.

Im Übrigen wird auf den als „GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 2b:

Es wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Antwort zu Frage 1e genannten Gründen nicht möglich.

Zu 2c:

Die „IMSI-Catcher“ der BPOL wurden ausschließlich in strafprozessualen Ermittlungsverfahren eingesetzt. Von der Umsetzung der richterlichen Beschlüsse gemäß § 100i Strafprozessordnung (StPO) waren insgesamt 52 Beschuldigte betroffen.

Im zweiten Halbjahr 2019 setzte das BKA den „IMSI-Catcher“ in neun abgeschlossenen Ermittlungsverfahren im Rahmen der Strafverfolgung ein, von denen 14 Personen betroffen waren.

In Verfahren des GBA wurden in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofs im zweiten Halbjahr 2019 „IMSI-Catcher“ zum Zwecke der Strafverfolgung in 15 Ermittlungsverfahren gegen 20 Betroffene eingesetzt.

Im Übrigen wird auf die als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ sowie „GEHEIM“ eingestufteten Antwortteile gemäß der Vorbemerkung verwiesen.

Zu 2d:

In den in der Antwort zu Frage 2c genannten Fällen, in denen in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofes „IMSI-Catcher“ in Ermittlungsverfahren des GBA eingesetzt wurden, wurde bislang kein Betroffener benachrichtigt. In diesen Fällen handelt es sich um laufende Ermittlungsverfahren, in denen die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegensteht.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den weiteren jeweils zuständigen Staatsanwaltschaften. Ob bzw. wie oft dies geschehen ist, ist der Bundesregierung nicht bekannt.

Betroffene von Beschränkungsmaßnahmen des BfV werden gemäß der §§ 9 Absatz 4 Satz 7, 8b Absatz 7 Satz 1 BVerfSchG i. V. m. § 12 G10 unterrichtet. Gleiches gilt für den MAD, für dessen Maßnahmen gemäß § 5 MADG die aufgeführten Vorschriften entsprechende Anwendung finden.

Zu 2e:

Betreffend die Maßnahmen aus dem vorigen Halbjahr, in denen in Umsetzung entsprechender Beschlüsse des Ermittlungsrichters des Bundesgerichtshofes „IMSI-Catcher“ in Ermittlungsverfahren des GBA eingesetzt wurden, wurden vier Betroffene nachträglich benachrichtigt. Im Übrigen sind die Betroffenen der Maßnahmen in Ermittlungsverfahren des GBA aus dem ersten Halbjahr 2019 bislang nicht nachträglich benachrichtigt worden. In diesen Fällen handelt es sich um laufende Ermittlungsverfahren, in denen die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegensteht.

Die Benachrichtigung der Person, die im ersten Halbjahr 2019 vom Einsatz des IMSI-Catchers in einem abgeschlossenen Gefahrenabwehrvorgang des BKA betroffen war, wurde nach § 74 Absatz 2 Bundeskriminalamtgesetz (BKAG) zurückgestellt.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den weiteren jeweils zuständigen Staatsanwaltschaften. Ob bzw. wie oft dies geschehen ist, ist der Bundesregierung nicht bekannt.

Im Übrigen wird auf den als GEHEIM eingestufteten Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 2f:

Grundsätzlich wird darauf hingewiesen, dass durch den Einsatz eines „IMSI-Catchers“ lediglich IMSI-Nummern sowie die IMEI erhoben werden und auf dieser Grundlage die dazugehörige deutsche Rufnummer ermittelt werden kann. Damit allein werden jedoch keine Straftaten aufgeklärt oder Gefahren abgewehrt. Vielmehr ist der Einsatz eines „IMSI-Catchers“ ein wesentlicher Ausgangspunkt für weitere Maßnahmen, wie z. B. die Erhebung von Verbindungsdaten, Ortungsmaßnahmen, OSINT-Recherchen und der Austausch mit Partnerbehörden. Erst dadurch können Sachverhalte inhaltlich weiter aufgeklärt werden.

Darüber hinaus ist die Aufklärung von Straftaten bzw. die Abwehr von Gefahren abhängig von verschiedenen Faktoren. Welche Maßnahmen wesentlich zur Aufklärung einer Straftat oder zur Abwehr einer Gefahr beigetragen haben, ist von Fall zu Fall unterschiedlich und kann in vielen Fällen nicht genau bestimmt werden. Bei einigen der im abgefragten Zeitraum liegenden Verfahren handelt es sich um noch laufende Ermittlungen oder um teils noch nicht abgeschlossene gerichtliche Verfahren, so dass es in diesen Fällen nicht möglich ist, die Maßnahmen zu benennen, die wesentlich zur Aufklärung der jeweiligen Straftat beigetragen haben.

Die Maßnahme des Einsatzes des „IMSI-Catchers“ dient zur Erforschung des Sachverhaltes und/oder der Ermittlung des Aufenthaltsortes des Beschuldigten oder im Gefahrenabwehrvorgang Polizeipflichtigen.

Der Entscheidung des jeweils zuständigen Gerichts über die Anordnung dieser Maßnahme lagen Sachverhalte zu Straftaten von auch im Einzelfall erheblicher Bedeutung (§ 100i StPO) oder Sachverhalte, die die Abwehr von dringenden Gefahren für die in der Norm genannten Rechtsgüter (§ 53 i.V.m. § 5 BKAG) bedingten, zugrunde. Die Ermittlung der Kommunikationsmittel und der Aufenthaltsorte der Täter oder Teilnehmer einer solchen Straftat oder des in einem Gefahrenabwehrvorgang Polizeipflichtigen sind daher grundsätzlich wesentlich.

Durch den Einsatz eines „IMSI-Catchers“ in Ermittlungsverfahren des GBA konnten der Sachaufklärung dienende Erkenntnisse gewonnen werden.

Zu 2g:

Im fragegegenständlichen Zeitraum wurden keine Ausfuhrgenehmigungen für sogenannte „IMSI-Catcher“ erteilt.

Zu 2h:

Es wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Frage 3:

Welche Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr sind derzeit technisch und rechtlich in der Lage, an Mobiltelefone sogenannte „Stille SMS“ zum Ausforschen des Standortes ihrer Besitzer/innen oder dem Erstellen von Bewegungsprofilen zu verschicken bzw. welche Änderungen haben sich gegenüber dem vorigen Halbjahr ergeben?

- a) Welche Bundesbehörden haben zwar selbst keine „Stillen SMS“ eingesetzt, sich hierfür aber anderer Behörden oder Firmen bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?*
- b) Wie viele „Stille SMS“ wurden von den jeweiligen Behörden im zweiten Halbjahr 2019 bzw. in deren Auftrag durch andere Behörden oder Firmen insgesamt jeweils versandt (bitte bezüglich des Zollkriminalamts nach den einzelnen Zollfahndungsämtern aufschlüsseln)?*
- c) Wie viele Personen und Ermittlungsverfahren waren jeweils betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?*
- d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?*
- e) Ist die Bundesregierung, sofern sie die Zahlen zu „Stillen SMS“ des BfV weiterhin als „VS – Geheim“ einstuft, bereit, dem Bundestag wenigstens abstrahierte Informationen hierzu offen zu übermitteln und zugleich in der Geheimschutzstelle des Bundestages konkretere, aber eingestufte Informationen zu hinterlegen?*
- f) Welche Hard- und Software wird von den Behörden zum Versand und zur Auswertung von „Stillen SMS“ genutzt bzw. welche Änderungen haben sich hierzu gegenüber dem vorigen Halbjahr ergeben (Drucksache 18/7285)?*

Zu 3:

Für die von dieser Kleinen Anfrage betroffenen Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes, einschließlich der Nachrichtendienste des Bundes, wird auf die Antwort der Bundesregierung zu Frage 4 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/7847 verwiesen, zu der sich im fragegegenständlichen Zeitraum keine Änderungen ergeben haben.

Zu 3a:

Die Anzahl der Ermittlungsverfahren, der versandten „Stillen SMS“ und der Betroffenen wird beim GBA nicht gesondert statistisch erfasst.

Für den Zoll wird auf die Antwort der Bundesregierung zu Frage 4a der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/12465 vom 16. August 2019 verwiesen, zu der sich im fragegegenständlichen Zeitraum keine Änderungen ergeben haben. Hinsichtlich der Zahlen des Zolls wird auf die Antwort zu Frage 3b verwiesen.

Darüber hinaus wird auf den als „GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 3b:

Im zweiten Halbjahr 2019 wurden durch die BPOL 27.778 sowie durch das BKA 34.938 „Stille SMS“ versandt.

Im Übrigen wird auf die als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ sowie „GEHEIM“ eingestuften Antwortteile gemäß der Vorbemerkung verwiesen.

Zu 3c:

Der Versand der „Stillen SMS“ durch das BKA betraf zwölf Ermittlungsverfahren im Rahmen der Strafverfolgung.

Darüber hinaus können weitere Angaben über die Anzahl betroffener Personen und Ermittlungsverfahren mangels statistischer Erfassung nicht gemacht werden.

Im Übrigen wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 3d:

Soweit beim BfV oder beim MAD ein Einsatz „Stiller SMS“ im Rahmen durch die G10-Kommission für zulässig und notwendig erklärter Beschränkungsmaßnahmen stattfindet, sind betroffene Personen entsprechend §12 G10 über die Beschränkungsmaßnahme zu benachrichtigen. Eine separate maßnahmenbezogene Erhebung von versendeten „Stillen SMS“ erfolgt nicht.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den jeweils zuständigen Staatsanwaltschaften. Ob bzw. wie oft dies geschehen ist, ist der Bundesregierung nicht bekannt.

Zu 3e:

Die Bundesregierung ist bereit, eine abstrahierte Aussage hinsichtlich des in Rede stehenden Sachverhalts zu übermitteln. Insofern wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestufteten Antwortteil gemäß der Vorbemerkung verwiesen.

Zu 3f:

Es wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestufteten Antwortteil gemäß der Vorbemerkung verwiesen.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Antwort zu Frage 1e genannten Gründen nicht möglich.

Frage 4:

Wie viele Maßnahmen der Funkzellenauswertung haben welche Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 vorgenommen (bitte wie in Drucksache 17/14714 beantworten)?

- a) Welche Bundesbehörden haben zwar selbst keine Maßnahmen der Funkzellenauswertung eingesetzt, sich hierfür aber der Amtshilfe anderer Behörden bedient (bitte außer den Zahlen auch die beteiligten Behörden benennen)?*
- b) Wie viele Anschlüsse, Personen und Ermittlungsverfahren waren jeweils insgesamt betroffen?*
- c) Welche der Funkzellenabfragen wurden vom Ermittlungsrichter des Generalbundesanwalts beim Bundesgerichtshof gestattet und im Zusammenhang mit welchen Ermittlungen fanden diese statt?*
- d) Wie viele Betroffene sind über die Maßnahmen nachträglich benachrichtigt worden (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?*
- e) Wie viele Betroffene der Maßnahmen aus dem vorigen Halbjahr sind über die Maßnahmen mittlerweile nachträglich benachrichtigt worden?*
- f) Inwiefern haben die Maßnahmen aus dem zweiten Halbjahr 2019 aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitrugen?*

Zu 4:

Im zweiten Halbjahr 2019 wurde durch das BKA in bereits abgeschlossenen Ermittlungsverfahren in drei Fällen Gebrauch von der Maßnahme der Funkzellenauswertung gemacht. Durch die BPOL wurden in 96 und durch den Zoll in 44 Fällen Funkzellenauswertungen durchgeführt.

Der BND, das BfV sowie der MAD besitzen keine Rechtsgrundlage zur Durchführung von Funkzellenabfragen und haben somit keine solchen Maßnahmen durchgeführt.

Zu 4a:

Im zweiten Halbjahr 2019 wurden in drei Ermittlungsverfahren des GBA elf Funkzellenauswertungen durch das BKA und das Polizeipräsidium Hessen durchgeführt. Der Zoll hat in fünf Fällen Amtshilfe des Landeskriminalamtes Rheinland-Pfalz zur Funkzellenauswertung in Anspruch genommen.

Zu 4b:

Betroffen waren in den unter 4a benannten Verfahren des GBA vier Beschuldigte. Von den Maßnahmen des BKA waren im fragegegenständlichen Zeitraum zwei Personen in einem Ermittlungsverfahren im Rahmen der Strafverfolgung betroffen. Weitere Angaben können mangels statistischer Erfassung nicht gemacht werden.

Zu 4c:

Die Maßnahmen des GBA erfolgten in Umsetzung von Beschlüssen des Ermittlungsrichters des Bundesgerichtshofs. Die Ermittlungen betreffen die Tatvorwürfe der Mitgliedschaft in einer kriminellen Vereinigung, der Mitgliedschaft in einer terroristischen Vereinigung im Ausland und des Mordes.

Die entsprechenden Erhebungen des BKA wurden durch den zuständigen Ermittlungsrichter am Bundesgerichtshof im Zuge der Ermittlungen im Bereich der politisch motivierten Kriminalität -links- angeordnet.

Zu 4d:

Die in den Ermittlungsverfahren des GBA Beschuldigten sind bislang nicht benachrichtigt worden. Es handelt sich um laufende Ermittlungsverfahren, in denen die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegensteht.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den jeweils zuständigen Staatsanwaltschaften. Ob bzw. wie oft dies geschehen ist, ist der Bundesregierung nicht bekannt.

Zu 4e:

Der Betroffene der Maßnahmen des GBA aus dem vorigen Halbjahr ist über die Maßnahme bislang nicht benachrichtigt worden. Es handelt sich um ein laufendes Ermittlungsverfahren, in dem die Gefährdung des Ermittlungszwecks einer Benachrichtigung derzeit noch entgegensteht.

Darüber hinaus obliegt die fragegegenständliche Benachrichtigung von Betroffenen den jeweils zuständigen Staatsanwaltschaften. Ob bzw. wie oft dies geschehen ist, ist der Bundesregierung nicht bekannt.

Zu 4f:

Grundsätzlich ist die Aufklärung von Straftaten bzw. die Abwehr von Gefahren abhängig von verschiedenen Faktoren. Welche Maßnahmen wesentlich zur Aufklärung einer Straftat oder zur Abwehr einer Gefahr beigetragen haben, ist von Fall zu Fall unterschiedlich und kann in vielen Fällen nicht genau bestimmt werden. Bei einigen der im abgefragten Zeitraum liegenden Verfahren handelt es sich um noch laufende Ermittlungen oder um teils noch nicht abgeschlossene gerichtliche Verfahren, so dass es in diesen Fällen nicht möglich ist, die Maßnahmen zu benennen, die wesentlich zur Aufklärung der jeweiligen Straftat beigetragen haben.

Die Maßnahme der Funkzellenauswertung dient der Erforschung des Sachverhaltes und/oder der Ermittlung von Tatverdächtigen und des Aufenthaltsortes des Beschuldigten oder im Gefahrenabwehrvorgang Polizeipflichtigen. Der Entscheidung der zuständigen Gerichte über die Anordnung dieser Maßnahme liegen grundsätzlich Sachverhalte zu Straftaten von auch im Einzelfall erheblicher Bedeutung oder die Abwehr von dringenden Gefahren zugrunde. Die Ermittlung der Kommunikationsmittel und der Aufenthaltsorte der Täter oder Teilnehmer einer solchen Straftat oder des in einem Gefahrenabwehrvorgang Polizeipflichtigen sind daher grundsätzlich wesentlich.

Durch die Maßnahmen in den in der Antwort auf Frage 4a benannten Ermittlungsverfahren des GBA konnten der Sachaufklärung dienende Erkenntnisse gewonnen werden.

Frage 5:

In welchem Umfang haben Bundesbehörden im zweiten Halbjahr 2019 geolokalisierte Standortdaten von Mobiltelefonen bei Herstellern der Geräte bzw. der Betriebssysteme abgefragt (bitte für BKA, Bundespolizei, BfV, Zollkriminalamt darstellen)?

Zu 5:

Das BKA, die BPOL sowie der Zoll haben keine derartigen Abfragen durchgeführt. Hinsichtlich des BfV ist eine Beantwortung aus den in der Antwort zu Frage 6 genannten Gründen nicht möglich.

Frage 6:

Inwiefern sind Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr 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 vorigen Halbjahr ergeben?

Zu 6:

Hinsichtlich des Zolls, des BKA und der BPOL wird auf die Antwort der Bundesregierung zu Frage 10 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/12465 vom 16. August 2019 verwiesen, zu der sich im fragegegenständlichen Zeitraum keine Änderungen ergeben haben.

Mit Blick auf die Nachrichtendienste des Bundes betrifft die Frage solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufteter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung findet seine Grenzen in den gleichfalls Verfassungsrang genießenden schutzwürdigen Interessen des Staatswohls.

Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf deren künftige Aufgabenerfüllung besonders schutzwürdig.

Eine Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Nachrichtendienste des Bundes einem nicht eingrenzbaeren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Bereits die Auskunft darüber, ob die genannten Behörden zur Durchführung des beschriebenen Verfahrens im Bereich der informationstechnischen Überwachung befähigt sind, lässt Rückschlüsse auf die Leistungsfähigkeit der Nachrichtendienste des Bundes zu. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen erheblichen Nachteil für deren wirksame Aufgabenerfüllung und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die vorgenannten Informationen über Tätigkeiten und aktive und ggf. zukünftige Fähigkeiten der Nachrichtendienste des Bundes wären geeignet, die künftige Möglichkeit der betroffenen Behörden zur Gewinnung von Erkenntnissen im Wege der technischen Aufklärung, in erheblicher Weise negativ zu beeinflussen. Die Informationsgewinnung durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung und Funktionsfähigkeit der Nachrichtendienste des Bundes jedoch unerlässlich. Zur Erstellung möglichst vollständiger Lagebilder und zur Vermeidung von Informationsdefiziten sind die Nachrichtendienste auf die aus der technischen Aufklärung zu generierenden Informationen zwingend und zunehmend angewiesen. Diese stellen einen unentbehrlichen Beitrag zum Informationsaufkommen dar. Das sonstige Informationsaufkommen der Nachrichtendienste des Bundes wäre auch nicht ausreichend, um ein vollständiges Lagebild zu erhalten und Informationsdefizite im Bereich der technischen Aufklärung zu kompensieren. Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen technischen Fähigkeiten bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und technische Fähigkeiten der Nachrichtendienste des Bundes sowie die Entwicklung derselben in den vergangenen Jahren gewinnen. Diese Kenntnisse würden es ihnen ermöglichen, ihr Kommunikationsverhalten so zu verändern, dass eine zukünftige Erhebung dieser Daten zumindest erschwert und in vielen Fällen in Gänze vereitelt werden würde. Dies wiederum würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, wodurch letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes nicht mehr sachgerecht erfüllt werden könnte.

Sofern derartige Informationen wegfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Damit wäre das Staatswohl der Bundesrepublik Deutschland gefährdet.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimchutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung der Nachrichtendienste Bundes nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Die angefragten Inhalte beschreiben die technischen Fähigkeiten der Nachrichtendienste des Bundes in einem Detaillierungsgrad, dass eine Bekanntgabe 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 Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt und einer Beantwortung der Kleinen Anfrage im Hinblick auf die Nachrichtendienste des Bundes im aktuellen Fall sowie (bei gleichlautender Anfrage und unverändertem Sachverhalt) in Zukunft entgegensteht. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

Frage 7:

Wie oft haben Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 Trojaner-Programme bzw. ähnliche Überwachungssoftware eingesetzt oder einsetzen lassen (bitte jeweils aufschlüsseln nach Polizei, Zoll, Geheimdiensten)?

- a) Welche der verfügbaren Programme (etwa „Übergangslösung“, Trojaner zur „Online-Durchsuchung“, Trojaner zur „Quellen-TKÜ“) kam dabei jeweils zur Anwendung?
- b) In welchem Umfang haben Bundesbehörden im vergangenen Halbjahr Trojaner auf mobilen Geräten platziert?
- c) Wie viele Personen und Ermittlungsverfahren waren von den Einsätzen der Trojaner insgesamt betroffen (bitte differenzieren in Informationsgewinnung, Gefahrenabwehr und Strafverfolgung)?
- d) Wie viele Betroffene sind hierüber nachträglich benachrichtigt worden?
- e) Inwiefern haben die Maßnahmen aus Sicht der Bundesregierung Erkenntnisse geliefert, die wesentlich zur Aufklärung von Straftaten bzw. Gefahren beitragen?

Zu 7, 7a bis 7e:

Die Fragen 7, 7a-7e werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Begriff „Trojaner“ ist zur Bezeichnung von Software zur Durchführung von Maßnahmen der informationstechnischen Überwachung, wie bspw. Quellen-TKÜ oder Online-Durchsuchung, im Allgemeinen ungeeignet.

Darüber hinaus wird auf den als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuftten Antwortteil gemäß der Vorbemerkung verwiesen.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Antwort zu Frage 6 genannten Gründen nicht möglich.

Frage 8:

In welchem Umfang haben die Behörden des Bundesministeriums des Innern, für Bau und Heimat, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums der Finanzen, des Bundeskanzleramtes und der Bundeswehr im zweiten Halbjahr 2019 die Möglichkeit genutzt, sich Zugang auf Nutzeraccounts bei den Messengerdiensten Signal, WhatsApp, Telegram oder vergleichbaren Anwendungen zu verschaffen, indem sich Ermittlerinnen oder Ermittler dort mit einem weiteren Gerät zum Mitlesen einloggen?

Zu 8:

Es wird auf die als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ sowie „GEHEIM“ eingestuften Antwortteile gemäß der Vorbemerkung verwiesen.

Frage 9:

Worin unterscheidet sich eine „Vordertür“ („Frontdoor“), wie sie der Präsident des Bundeskriminalamtes zum staatlichen Zugang zu verschlüsselter Ende-zu-Ende-Telekommunikation ins Gespräch bringt („Crypto Wars: BKA-Chef will ‚Frontdoor-Debatte‘ führen‘, www.heise.de vom 23. November 2019), von einer „Hintertür“ („Backdoor“), mit der die Betreiber zur „Herausgabe einer unkryptierten Überwachungskopie“ verpflichtet werden könnten (bitte die technischen und rechtlichen Unterschiede erläutern; vgl. auch „Interpol group delays criticism of encryption after objections“, Reuters vom 27. November 2019), und welche politischen Initiativen auf Ebene der Europäischen Union sind der Bundesregierung wie vom BKA-Präsidenten erwähnt zu einer solchen „Frontdoor-Debatte“ bekannt?

Zu 9:

Die Begriffe der „Frontdoor“ und „Backdoor“ sind nicht wörtlich auszulegen und beruhen auch nicht auf einer juristischen Diktion. Im Unterschied zu einer „Backdoor“ beschreibt die hier zitierte „Frontdoor“-Lösung den gesetzlich legitimierte Zugang der Sicherheitsbehörden zu unverschlüsselten Kommunikationsinhalten, einhergehend mit der Verpflichtung des Anbieters, unverschlüsselt ausleiten zu müssen. Insofern zielt der Begriff auf eine (gesetzlich zu verankernde) aktive Mitwirkungspflicht des Anbieters ab. So verpflichtet das Telekommunikationsgesetz (TKG) derzeit die Betreiber von Telekommunikationsanlagen, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden, technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten.

Da heute der größte Teil der Kommunikation jedoch verschlüsselt erfolgt, stößt die bestehende Regelung an Grenzen. Um den dadurch bedingten Informationsverlust auszugleichen, ist die Option einer unverschlüsselten Ausleitung („Frontdoor“), in Ergänzung zur bestehenden Rechtslage, vom Präsidenten des BKA angesprochen worden.

Der Schutz der Vertraulichkeit der Kommunikation durch Verschlüsselung einerseits und die fortdauernde Sicherstellung der Ermittlungsfähigkeiten der deutschen Sicherheitsbehörden in der digitalen Welt andererseits sind hohe gesellschaftliche Güter, deren Belange sorgsam abzuwägen sind. Diese Abwägung hat die Bundesregierung im Kryptoeckwertebeschluss niedergelegt.

Die Bundesregierung strebt weiterhin keine Hintertüren („Backdoors“) oder Verschlüsselungsverbote an. Geboten ist aber ebenfalls die Aufrechterhaltung der TKÜ-Fähigkeiten der Sicherheitsbehörden.

Erwägenswert ist daher die Erarbeitung eines klaren und technikneutralen Ansatzes, der eine Lösung dieser Herausforderung aufzeigt. Die Bundesregierung steht hier noch am Anfang einer Lösungsfindung, die gemeinsam und im Dialog mit allen Beteiligten erarbeitet werden wird.

Diese Auffassung wird durch das BKA auch auf europäischer Ebene vertreten.

Frage 10:

Mit welchen Anfragen hat sich das BKA in der Vergangenheit an die „Entschlüsselungsplattform“ bei Europol gewandt bzw. Unterstützung erfolgte von der Abteilung in Ermittlungsverfahren (Antwort auf die Bundestagsdrucksache 19/15217, Frage 8)?

- a) Welche Geräte (etwa Speichermedien, Rechner, Telefone), Anwendungen (Software oder Apps) oder Verfahren können von der „Entschlüsselungsplattform“ entschlüsselt werden?*
- b) Seit wann hat die „Entschlüsselungsplattform“ mit diesen Unterstützungsmaßnahmen begonnen und wie häufig wird sie vom BKA angefragt?*

Zu 10:

Das BKA hat sich in der Vergangenheit in sechs Fällen mit Entschlüsselungsaufträgen an die „Entschlüsselungsplattform“ gewandt.

Zu 10a:

Das Portfolio an unterstützten Geräten, Anwendungen oder Verfahren ist der Bundesregierung im Detail nicht bekannt.

Zu 10b:

Nach Kenntnis der Bundesregierung wurde die „Entschlüsselungsplattform“ im Jahr 2014 durch Europol in Betrieb genommen. Seitens des BKA wurden insgesamt sechs Anfragen an die „Entschlüsselungsplattform“ gerichtet.

Frage 11:

Welche Soft- und Hardware haben das Bundesministerium der Verteidigung, das Bundeskanzleramt oder dem Bundesinnenministerium nachgeordnete Sicherheitsbehörden für die Überwachung öffentlich zugänglicher Quellen und geschlossener Foren im Internet beschafft bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12456 ergeben?

Zu 11:

Die Bundesregierung legt ihrer Antwort auf diese Kleine Anfrage das in der Vorbemerkung und das zu Frage 12 der vorerwähnten Bundestagsdrucksache mitgeteilte Verständnis zu Grunde und bezieht ihre Antwort ausschließlich auf die Strafverfolgungs-, Ermittlungs- und Gefahrenabwehrbehörden des Bundes, einschließlich der Nachrichtendienste des Bundes.

Es haben sich keine Änderungen gegenüber der Antwort der Bundesregierung zu Frage 13 auf die Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 19/12465 vom 16. August 2019) ergeben.

Frage 12:

Welche „Methoden der Computerlinguistik und der Künstlichen Intelligenz“ haben das Bundesministerium der Verteidigung, das Bundeskanzleramt oder dem Bundesinnenministerium nachgeordnete Sicherheitsbehörden im zweiten Halbjahr 2019 zum Abgleich genutzt bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12465 ergeben?

Zu 12:

Es haben sich keine Änderungen gegenüber der Antwort der Bundesregierung zu Frage 15 auf die Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 19/12465 vom 16. August 2019) ergeben.

Frage 13:

Welche „Methoden des maschinellen Lernens“ wurden im Bundeskriminalamt im zweiten Halbjahr 2019 „im Einzelfall anlassbezogen“ auf Datenbestände von Ermittlungsverfahren angewendet bzw. welche Änderungen haben sich gegenüber der Bundestagsdrucksache 19/12465 ergeben?

Zu 13:

Es haben sich keine Änderungen gegenüber der Antwort der Bundesregierung zu Frage 16 auf die Kleine Anfrage der Fraktion DIE LINKE. (Bundestagsdrucksache 19/12465 vom 16. August 2019) ergeben.