Kleine Anfrage des Abgeordneten Jan Korte und der Fraktion DIE LINKE.

Ermittlungen gegen eine deutsch-britische Software-Firma wegen illegaler Überwachung von Oppositionellen in Bahrain und Deutschland

BT-Drucksache 18/3852

Vorbemerkung der Fragesteller:

Das European Center for Constitutional and Human Rights (ECCHR) und die britische Organisation Privacy International haben Anhaltspunkte, wonach bahrainische Behörden unter anderem auch in Deutschland lebende Oppositionelle mithilfe des Gamma-Trojaners FinFisher unrechtmäßig ausgespäht haben. Am 16. Oktober 2014 haben die Organisationen deshalb bei der Staatsanwaltschaft München Strafanzeige gegen Mitarbeiter des deutsch-britischen Konzerns Gamma eingereicht. Den Organisationen liegen Datensätze vor, die den Verdacht begründen, dass Gamma die Überwachungssoftware FinFisher nach Bahrain lieferte sowie technische Hilfe von Deutschland aus leistete. Dadurch konnten laut ECCHR bahrainische Behörden den Trojaner nutzen, um Computer in Deutschland auszuspähen. Die Staatsanwaltschaft hat eine entsprechende Ermittlungsaufnahme indes abgelehnt, obwohl aus Wikileaks-Dokumenten (www.wikileaks.org/spyfiles4/database.html) entsprechende Hinweise und Informationen hervorgehen. Weitere Hinweise, insbesondere zur Situation in Bahrain und zum Einsatz des Gamma-Trojaners FinFisher, lassen sich in etlichen Dokumenten auf der Homepage der Nichtregierungsorganisation Bahrain Watch finden (vgl. www.bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/). Laut Miriam Saage-Maaß, der stellvertretenden Legal Director des ECCHR, werden in Bahrain Menschenrechtsaktivisten, Journalisten und Oppositionelle systematisch überwacht, verfolgt, inhaftiert und immer wieder auch gefoltert. „Angesichts der Überwachungsrealität in Bahrain ist es absurd, zu sagen, staatliche Behörden könnten gar nicht ‚hacken' und gegen § 202 a StGB (Strafgesetzbuch) – dem Verbot der Ausspähung von Daten – verstoßen" (Pressemitteilung des ECCHR vom 12.12.2014). Die Staatsanwaltschaft München erklärte in ihrem Schreiben an das ECCHR vom 28.11.2014 unter Punkt 2aa), dass das Vorbereiten des Ausspähens von Daten gemäß § 202c StGB generell nicht die Herstellung und den Vertrieb von Software zur Datenerhebung durch staatliche Stellen erfasst, unabhängig davon, ob die Datenerhebung durch den Staat mithilfe der Software rechtmäßig erfolgt.

Nach Informationen des ECCHR geht aus Daten von 77 Computern hervor, dass bahrainische Behörden mit dem Trojaner neben Geräten in Großbritannien auch je

einen Computer in Belgien und Deutschland ausgespäht haben. In Großbritannien waren davon unter anderem prominente bahrainische Menschenrechtsaktivisten betroffen. Die Identität der in Deutschland ausspionierten Person ist bisher nicht bekannt.
Auch in Großbritannien und Belgien liegen derzeit Strafanzeigen gegen die Firma Gamma International, die FinFisher entwickelt und produziert hat, vor.
Werbematerial der Firma zeigt, dass die Software den umfassenden Zugriff auf infizierte Geräte und alle enthaltenen Daten ermöglicht. Dazu gehört auch, dass Kameras und Mikrofone an Computern angezapft werden können. Laut Privacy International wird FinFisher-Software in 35 Ländern, darunter Äthiopien, Turkmenistan, Bahrain und Malaysia, eingesetzt.
Da selbst das Bundeskriminalamt mindestens bis 2012 auf den Einsatz einer Version des Gamma-Trojaners verzichtete, weil die Software gegen die „standardisierende Leistungsbeschreibung" der Bundesregierung (www.netzpolitik.org vom 21. August 2014 „Geheimes Dokument: Bundeskriminalamt darf FinFisher FinSpy nicht einsetzen, versucht einfach neue Version nochmal") und damit gegen verfassungsrechtliche Mindeststandards verstieß, wirft das ECCHR der Staatsanwaltschaft München außerdem vor, durch die Entscheidung keine Ermittlungen gegen Gamma International einzuleiten, die Rechtslage in Deutschland zu ignorieren.

Vorbemerkung:
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 13, 14, 15, 16 und 17 aus Geheimhaltungsgründen ganz oder teilweise nicht oder nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden können. Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die Einstufung der Antworten auf die Fragen 13, 14, 15, 16 und 17 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 - insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden - einem nicht eingrenzbaren Personenkreis 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" (VS-NfD) eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Haben die Bundesregierung und deutsche Sicherheitsbehörden Kenntnis über die Ausspähung in der Bundesrepublik Deutschland lebender Oppositioneller mithilfe des Gamma-Trojaners FinFisher? Wenn ja, durch wen erfolgt die Überwachung und wer ist davon betroffen?

Zu 1.

Der Bundesregierung liegen hierzu keine über die diesbezügliche Medienberichterstattung hinausgehenden Erkenntnisse vor.

2. Ist der Bundesregierung bekannt, ob auch Rechner und Informationssysteme von an Asylverfahren beteiligten Einrichtungen, vor allem des Bundes, Ziel der Ausspähung durch Geheimdienste von Staaten sind, die Oppositionelle verfolgen?

a) Sind der Bundesregierung derartige Angriffe bekannt, und wenn ja, auf welche Einrichtungen sind diese wann, von wem und mit welchem Ziel jeweils erfolgt, und welche Konsequenzen seitens der Sicherheitsbehörden, des Bundesamts für Sicherheit in der Informationstechnik oder des Bundesamtes für Verfassungsschutzes hatte dies jeweils?

b) Sind der Bundesregierung grundsätzlich Angriffe auf die Kommunikationsinfrastruktur des Bundes bekannt, die mit Produkten der Gamma-Firmengruppe verübt wurden?

Zu 2 a

Der Bundesregierung ist bekannt, dass eine Vielzahl von Stellen des Bundes von elektronischen Angriffen mit vermutlich nachrichtendienstlichem Hintergrund betroffen sind, darunter auch an Asylverfahren beteiligte Einrichtungen des Bundes wie beispielsweise das Bundesamt für Migration und Flüchtlinge (BAMF), das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung und das Auswärtige Amt. Es sind bisher nur Mutmaßungen darüber möglich, wer diese Angriffe mit welcher Zielsetzung initiierte. Ein spezieller Zusammenhang mit der durch bestimmte fremde Nachrichtendienste betriebenen gezielten Ausspähung von Oppositionellen

ist bislang nicht ersichtlich.

Zu 2 b
Nein.

3. Wie beabsichtigt die Bundesregierung ihrer Schutzpflicht gegenüber ihren Bürgerinnen und Bürgern aber auch gegenüber Asylsuchenden in Deutschland nachzukommen, sie vor Zugriffen ausländischer Geheimdienste zu schützen?

Zu 3.
Die Bundesregierung ist sich der anhaltenden Bedrohung durch Spionage fremder Nachrichtendienste für Staat und Wirtschaft, aber auch für Bürgerinnen und Bürger gerade in Zeiten einer weiter zunehmenden digitalen Vernetzung bewusst. Um Bürgerinnen und Bürger besser vor Ausspähung privater und geschäftlicher Daten zu schützen - unabhängig davon, ob diese Ausforschung durch fremde Nachrichtendienste oder etwa kriminelle Hacker erfolgt - hat sich die Bundesregierung in der Digitalen Agenda zum Ziel gesetzt, Verschlüsselung von privater Kommunikation in der Breite zum Standard werden zu lassen und die Anwendung von Sicherheitstechnologien wie beispielsweise De-Mail auszubauen. Hierbei hat sich auch das Konzept der staatlichen Zertifizierung von im Wettbewerb angebotenen Produkten und Diensten auf Basis definierter Sicherheitsstandards durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewährt.

Die innerhalb der Bundesverwaltung für die Bearbeitung von Vorgängen im Zusammenhang mit Asylsuchenden zuständigen Behörden BAMF und Bundesverwaltungsamt (BVA) setzen ein Informationssicherheitsmanagement gemäß der Empfehlungen im „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) um und sind in die gesicherten IT-Infrastrukturen des Bundes eingebunden und somit besonders vor IT-Angriffen geschützt. Zur Durchführung des Asylverfahrens werden die Daten von Asylbewerbern beim BAMF in einer elektronischen Asylverfahrensakte (IT-System MARIS) vorgehalten, die nach den Vorgaben des UP Bund und denen des BSI gesichert ist. Das im BVA betriebene Ausländerzentralregister, in dem Daten von Ausländern zur Durchführung ausländer- oder asylrechtlicher Vorschriften vorgehalten werden, verfügt über keine Verbindung zum Internet und kommuniziert mit anderen Behörden und Stellen nur innerhalb der besonders gesicherten IT-Netzinfrastruktur der Verwaltung und dort nur mittels gesicherten Verbindungen. Die Mitarbeiter in diesem Aufgabenbereich sind sicherheitsüberprüft und arbeiten in besonderen Sicherheitsbereichen. Weitere Schutzmaßnahmen sind in Absprache mit dem BSI eingerichtet.

4. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus den auf der Wikileaks-Plattform veröffentlichten Dokumenten zur Gamma-Firmengruppe im Hinblick auf ihre Beweiskraft? Befürwortet die Bundesregierung, dass gegen das Unternehmen Ermittlungen erfolgen?

Zu 4.

Die Strafverfolgung obliegt in Deutschland grundsätzlich den Ländern. Die Bundesregierung hat in dieser Hinsicht keinerlei Weisungs- oder Aufsichtsrechte und kann insoweit weder die Beweiskraft einzelner Vorgänge einschätzen noch beurteilen, ob in bestimmten Einzelfällen Ermittlungen einzuleiten sind oder nicht. Die Beurteilung der Frage, ob zureichende tatsächliche Anhaltspunkte dafür vorliegen, ein Ermittlungsverfahren einzuleiten, ist Sache der zuständigen Staatsanwaltschaft.

5. Welche Maßnahmen wird die Bundesregierung in Bezug auf den Inhaber der IP-Adresse 217.86.164.76 ergreifen, der laut im August 2014 veröffentlichter Dokumente möglichweise seit 2011 in Deutschland vom bahrainischen Geheimdienst ausgespäht wird?

Zu 5.

Die (Medien-)Hinweise auf Ausspähaktivitäten durch fremde Geheimdienste unter Nutzung der Software "FinFisher" sind Gegenstand eines Beobachtungsvorgangs des Generalbundesanwalts beim Bundesgerichtshof, in dem geprüft wird, ob ein Anfangsverdacht einer geheimdienstlichen Agententätigkeit zu bejahen ist. Die Prüfungen sind jedoch noch nicht abgeschlossen.

6. Stimmt die Bundesregierung der Auffassung der Staatsanwaltschaft München zu, wonach das Vorbereiten des Ausspähens von Daten gemäß § 202c StGB generell nicht die Herstellung und den Vertrieb von Software zur Datenerhebung durch staatliche Stellen erfasst, unabhängig davon, ob die Datenerhebung durch den Staat mithilfe der Software rechtmäßig erfolgt?

Zu 6.

Die Einschätzung der Strafbarkeit des Verbreitens bestimmter Programme obliegt den dafür zuständigen Strafverfolgungsbehörden und Gerichten.

7. Ist die Bundesregierung Hinweisen darauf, dass Gamma International/FinFisher Labs GmbH kontinuierlich Updates an Bahrain liefert bzw. die Technologie wartet, nachgegangen (www.netzpolitik.org vom 2. August 2014 „Gamma FinFisher: Über-

wachungstechnologie „Made in Germany" gegen Arabischen Frühling in Bahrain eingesetzt(Update)" und www.spiegel.de vom 8. August 2014 „FinFisher-Software: Kundendienst half bei Überwachung in Bahrain")?

a) *Würden solche Wartungen im Zusammenhang mit Bahrain nach Ansicht der Bundesregierung einen Einzeleingriff nach § 6 des Außenwirtschaftsgesetzes (AWG) rechtfertigen bzw. gegen die geänderte europäische Verordnung (EG) Nr. 428/ 2009 (EG-Dual-Use-Verordnung) verstoßen?*
b) *Liegen der Bundesregierung entsprechende Anträge der Gamma- bzw. FinFisher Firmengruppe oder des Unternehmens Elaman vor?*

Zu 7.

Zur Exportkontrolle von Gütern der Überwachungstechnik hat die Bundesregierung in ihrer Beantwortung der Kleinen Anfrage der Fraktion BÜNDNIS 90 / DIE GRÜNEN „Haltung der Bundesregierung bezüglich der Effektivierung von Exportkontrollen für doppelverwendungsfähige Überwachungstechnologie und Zensursoftware", Bundestagsdrucksache 18/2374 vom 18. August 2014, ausführlich Stellung genommen. Dabei hat sich die Bundesregierung auch zu Lieferungen von Software durch die Firma Gamma nach Bahrain geäußert (vgl. Antwort der Bundesregierung zu Frage 10 der vorgenannten Kleinen Anfrage). Die Bundesregierung wird aufgrund von Kenntnissen tätig, die in regulären behördlichen Verfahren, insbesondere in Antragsverfahren für Ausfuhrgenehmigungen, gewonnen werden. Anträge der in der Frage angesprochenen Unternehmen zu Ausfuhren nach Bahrain liegen der Bundesregierung nicht vor. Aus den in der Frage zitierten Presseberichten ergeben sich darüber hinaus keine neuen Aspekte.

Ohne behördliche Kenntnis im dargelegten Sinne über die konkreten Güter oder diesbezüglichen Serviceleistungen kann eine rechtliche Prüfung nicht erfolgen. Grundsätzlich aber gilt: Die Bundesregierung wird bei entsprechender Kenntnis auch Ausfuhren, die keiner Genehmigungspflicht unterliegen, im Einzelfall mittels des Instruments des Einzeleingriffs nach § 6 des Außenwirtschaftsgesetzes (AWG) unterbinden, wenn durch diese Ausfuhren eine Gefahr für die in § 4 Absatz 1 AWG genannten Rechtsgüter bestünde. Auch in Bezug auf technische Unterstützung in Form von Wartungen, die nicht als eigenständige Ausfuhr qualifiziert werden können, prüft die Bundesregierung dies intensiv.

8. Wie viele Lieferungen von Überwachungstechnologie und Zensursoftware an Drittstaaten wurden im Zuge der von Bundesminister Sigmar Gabriel am 19. Mai 2014 angekündigten strengeren Kontrolle des Exportes von Überwachungstechnologie und Zensursoftware durch den Zoll auf Grundlage des Instruments des Ein-

zeleingriffs nach § 6 AWG untersagt (bitte mit Exportgut und Empfängerland konkret angeben)?

Zu 8.

Die im Rahmen des Wassenaar-Arrangements beschlossenen erweiterten Kontrollen bei Gütern der Überwachungstechnik, für die auf die Antwort zu Frage 1 der Kleinen Anfrage der Fraktion BÜNDNIS 90 / DIE GRÜNEN „Haltung der Bundesregierung bezüglich der Effektivierung von Exportkontrollen für doppelverwendungsfähige Überwachungstechnologie und Zensursoftware", Bundestagsdrucksache 18/2374 vom 18. August 2014 verwiesen wird, sind zwischenzeitlich in Kraft getreten. Vor Inkrafttreten dieser neuen Genehmigungspflichten hat die Bundesregierung keine Kenntnis von Ausfuhren erlangt, die nunmehr von einer dieser neuen Genehmigungspflichten erfasst wären und bis dahin einen Einzeleingriff nach § 6 AWG zu deren Verhinderung erforderlich gemacht hätten. Insofern wurden auch keine Lieferungen von Überwachungstechnik an Drittstaaten auf Grundlage des Instruments des Einzeleingriffs nach § 6 AWG durch die Zollverwaltung angehalten. Im Übrigen wird auf die Antwort zu Frage 7 verwiesen.

9. Wie viele Lieferungen von Überwachungstechnologie und Zensursoftware an Drittstaaten sind seit der Ankündigung des Bundesministers Sigmar Gabriel vom 19. Mai 2014 nach Kenntnis der Bundesregierung erfolgt (bitte mit Exportgut und Empfängerland konkret angeben)?

Zu 9.

Zur Definition von Überwachungstechnik wird auf die Antwort zu Frage 1 der Kleinen Anfrage der Fraktion BÜNDNIS 90 / DIE GRÜNEN „Haltung der Bundesregierung bezüglich der Effektivierung von Exportkontrollen für doppelverwendungsfähige Überwachungstechnologie und Zensursoftware", Bundestagsdrucksache 18/2374 vom 18. August 2014, verwiesen. Die in Deutschland seit dem 19. Mai 2014 erteilten Ausfuhrgenehmigungen und Nullbescheide zu Exporten von Gütern der Überwachungstechnik einschließlich von Gütern der Telekommunikationsüberwachung (TKÜ) in Drittländer (§ 2 Absatz 8 AWG) betreffen Anträge von Unternehmen, die in Deutschland niedergelassen sind. Hiermit ist nichts über die Ausnutzung der Ausfuhrgenehmigungen und Nullbescheide oder tatsächliche Lieferungen gesagt.

Gut	Bestimmungsland
Entschlüsselungseinrichtung für Satellitenkommunikationssystem	Ägypten
Entschlüsselungseinrichtung für Satellitenkommunikationssystem	Indien
Systemkomponenten für ein Monitoring Center	Indonesien
IMSI-Catcher	Marokko
IMSI-Catcher	Montenegro
SAP-Unternehmenssoftware mit Verschlüsselungsbibliothek	Nigeria
Entschlüsselungseinrichtung für Satellitenkommunikationssystem	Schweiz
Interception Center	Taiwan

10. Wie bewertet die Bundesregierung den Einsatz des FinFisher-Trojaners in Deutschland in rechtlicher Hinsicht?

Zu 10.

Nach dem Verständnis der Bundesregierung betrifft Frage 10 ausschließlich einen Einsatz der erwähnten FinFisher-Software durch fremde Staaten und nicht durch deutsche staatliche Stellen. Hierzu wird auf die Antwort zu Frage 4 verwiesen. Eine Einschätzung der Strafbarkeit des Einsatzes bestimmter Programme obliegt grundsätzlich den dafür zuständigen Strafverfolgungsbehörden und Gerichten.

11. Inwieweit treffen Berichte zu (www.sueddeutsche.de vom 15. April 2014 „Allianz gegen Feinde des Internets" und www.ndr.de vom 7. Dezember 2011 „Exporthilfe für Überwachungstechnologie"), dass es außer den zwei zugestandenen Hermesbürgschaften für Überwachungstechnologie in den Jahren 2005 und 2006 weitere Hermesbürgschaften für solche Software gegeben hat?

Zu 11.

In der Bundestagsdrucksache 18/2374 teilte die Bundesregierung mit, dass im Zeitraum von 2003 bis 2013 zwei Exportkreditgarantien für die Lieferung in Telekommunikationsprojekte nach Malaysia und Russland übernommen wurden, die auch Überwachungstechnik enthielten. Diese Übernahmen erfolgten im Jahr 2005. Darüber hinaus ist festzustellen, dass in den Jahren 2000 und 2001 Exportkreditgarantien für Ausfuhren von Überwachungstechnik nach Litauen übernommen wurden.

12. Wie erklärt die Bundesregierung ihre widersprüchlichen Angaben gegenüber den Bundestagsabgeordneten und der Presse zum Export von Überwachungssoftware (vgl. Süddeutsche Online vom 28.11.2014)?

Zu 12.

Die Angaben der Bundesregierung gegenüber Bundestagsabgeordneten und der Presse waren jederzeit konsistent und nicht widersprüchlich. In der Kleinen Anfrage der Fraktion BÜNDNIS 90/ DIE GRÜNEN „Haltung der Bundesregierung bezüglich der Effektivierung von Exportkontrollen für doppelverwendungsfähige Überwachungstechnologie und Zensursoftware" auf Bundestagsdrucksache 18/2067 wurde die Bundesregierung nach Ausfuhren in den Jahren 2003 bis 2013 gefragt. Die Recherche und die von der Bundesregierung in ihrer Antwort zu Frage 2 übermittelte Tabelle waren auf die Vorgaben der Bundestagsabgeordneten zugeschnitten. Daher bezog sich diese Frage lediglich auf Ausfuhren. Dies sind Lieferungen in Drittländer, also in Gebiete außerhalb des Zollgebiets der Europäischen Union. Gleichzeitig wies die Bundesregierung darauf hin, dass ihr keine Informationen zu getätigten Ausfuhren vorliegen. Zur Gewährleistung größtmöglicher Transparenz übermittelte die Bundesregierung nicht nur die ihr vorliegenden Informationen zu erteilten Ausfuhrgenehmigungen, sondern auch zu Nullbescheiden. Solche Nullbescheide genehmigen die Ausfuhr nicht, sondern stellen rechtsverbindlich fest, dass ein bestimmtes Vorhaben weder verboten noch genehmigungspflichtig ist.
Um bei im Wesentlichen gleich gelagerten Anfragen untereinander konsistente Zahlen herauszugeben, hat die Bundesregierung im Folgenden auch gegenüber der Presse auf Basis der genannten Tabelle geantwortet. Die von einem einzelnen Journalisten wahrgenommenen Abweichungen zu älteren Anfragen, die eine zwangsläufige Folge punktueller respektive unterschiedlich formulierter Anfragen sind und damit zu anderen Prämissen bei der Recherche führen, wurden durch die Bundesregierung gegenüber diesem Journalisten aufgeklärt.

13. Wann genau hat das Bundeskriminalamt von der Gamma- bzw. FinFisher-Firmengruppe den Staatstrojaner FinSpy 4.20 gekauft, wie hoch waren die Kosten, und wie oft wurde dieser mittlerweile eingesetzt?

Vorbemerkung zu den Fragen 13 bis 16:
Die Verwendung des Begriffs „Staatstrojaner" ist im Kontext der Fragestellung missverständlich. Als „Trojaner" wird im EDV-Jargon üblicherweise ein Computerprogramm bezeichnet, das als nützliche Anwendung getarnt ist, im Hintergrund ohne Wissen des Anwenders jedoch eine andere (aus Sicht des Anwenders gegebenenfalls unerwünschte, schädliche) Funktion erfüllt. Bei der durch das Bundeskriminalamt (BKA) beschafften Software handelt es sich um eine Software für die Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), die ausschließlich den Zweck der Ausleitung laufender Kommunikation der betroffenen Person von deren Endgerät - bei abgehender Kommunikation vor der Verschlüsselung beziehungsweise bei eingehender Kommunikation nach der Entschlüsselung - und insbesondere keine scheinbar nützlichen Funktionen zum Zwecke der Tarnung erfüllt.

Zu 13.
Es wird auf den VS-NfD eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

14. Sofern der Staatstrojaner FinSpy 4.20 nicht eingesetzt wurde, worin bestanden bzw. bestehen die Gründe?

15. Welche andere Version des FinSpy-Trojaners wurde bzw. wird im Bundeskriminalamt eingesetzt (bitte aufschlüsseln nach Version und Anzahl der eingesetzten Fälle)?

16. Inwiefern und mit welcher Begründung trifft es zu, dass die Firma CSC Solutions letztes Jahr festgestellt hatte, dass die Software in der Version 4.20 gegen deutsches Recht verstößt bzw. verstieß (www.netzpolitik.org vom 8. Januar 2015 „Informationsfreiheits-Ablehnung des Tages: Informationsfreiheits-Beauftragte lehnt Anfrage zu illegalen Trojaner ab")?

Zu 14. bis 16.
Es wird auf die Vorbemerkung zu den Fragen 13 bis 16 sowie auf den VS-NfD eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

17. Wird von CSC ein Vorschlag gemacht, wie der Einsatz der Version 4.20 technisch und rechtlich ermöglicht werden könnte, und wenn ja, wie sieht dieser aus?

Zu 17.
Es wird auf den VS-NfD eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

18. Aus welchen Gründen ist der CSC-Prüfbericht als geheim eingestuft, und wann wurde er wie dem Deutschen Bundestag zugänglich gemacht?

Zu 18.
Die Einstufung erfolgte nach Prüfung des Dokuments unter Maßgabe des § 3 VSA. Es handelt sich hier um eine verdeckte polizeiliche Einsatzmaßnahme, deren technische Funktionsweise aus einsatztaktischen und polizeifachlichen Gründen sensibel behandelt werden muss. Die Prüfung ergab, dass in dem Dokument unter anderem Informationen zur Funktionsweise von Quellen-TKÜ-Software enthalten sind. Eine Veröffentlichung dieser Informationen würde unter Umständen zur Wirkungslosigkeit beziehungsweise zumindest zu einer eingeschränkten Wirkung zukünftiger Maßnahmen der Quellen-TKÜ führen und hätte somit schweren Schaden für die (innere) Sicherheit der Bundesrepublik Deutschland zur Folge. Ein Einsatz der Software soll bei der Verfolgung schwerster Straftaten bzw. bei Gefahrenlagen zum Schutz von Leib und Leben erfolgen. Im Ergebnis wird diese Bewertung des BKA durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die im Rahmen einer diesbezüglichen Informationsfreiheitsgesetz-Anfrage von einem Petenten um Vermittlung gebeten wurde, geteilt.

Der Prüfbericht wurde den Abgeordneten des Deutschen Bundestages bislang noch nicht zugänglich gemacht. Der Prüfbericht kann bei Bedarf über die Geheimschutzstelle des Deutschen Bundestages dem dazu berechtigten Personenkreis zur Einsichtnahme zur Verfügung gestellt werden.