**Deutscher Bundestag** **Drucksache 19/1434**

**19. Wahlperiode** 28.03.2018

# Antwort

**der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Canan Bayram, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN**
**– Drucksache 19/982 –**

## Staatliches Hacking von Internetkommunikation – Transparenz rechtlicher und tatsächlicher Voraussetzungen

Vorbemerkung der Fragesteller

Die Kommunikation von Zivilgesellschaft und Wirtschaft findet zunehmend online statt. Die meist kommerziellen Angebote und Produkte waren und sind strukturell nicht primär auf Datensicherheit ausgelegt. Der Erhalt des Vertrauens in die Privatheit von Kommunikation ist rechtsstaatlich essentiell. In Wahrnehmung seiner Aufgaben der Sicherheitsverantwortung eröffnen sich Staaten durch die Digitalisierung mehr Überwachungsmöglichkeiten als je zuvor (vgl. dazu etwa Studie der Heinrich-Böll-Stiftung unter www.boell.de/sites/default/files/e-paper_internationalpolitik_verschluesselung.pdf?dimension1=startseite).
Zugleich treffen staatliche Stellen umfängliche Schutzpflichten zur Gewährleistung der Rechte auf Privatheit, auf Vertraulichkeit und Integrität informationstechnischer Systeme als auch zum Schutz des Telekommunikationsgeheimnisses. Denn diese Rechte zählen zu den Funktionsbedingungen freiheitlich-demokratischer Rechtsstaaten (vgl. etwa BVerfG, www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html). Die Snowden-Veröffentlichungen und die daraus resultierende parlamentarische Aufklärung, unter anderem auch im Deutschen Bundestag, haben nach Auffassung der Oppositionsfraktionen im 1. Untersuchungsausschuss der 18. Wahlperiode ein flächendeckend angelegtes internationales Netzwerk staatlicher Massenüberwachung internetgestützter Kommunikation durch westliche Geheimdienste offengelegt. Auch vor dem Hintergrund einer hohen Anfälligkeit gegenüber zunehmenden IT-Angriffen stellen Bestrebungen von Wirtschaft, Regierungen und Zivilgesellschaft, Kommunikationen durch Kryptographie und starke Verschlüsselungen vor unbefugter Kenntnisnahme zu schützen, wichtige und unterstützenswerte Schutzmaßnahmen dar. Dass diese Maßnahmen Herausforderungen für die Aufgabenwahrnehmung der Sicherheitsbehörden darstellen können, ist unbestritten.

Anhaltende Bestrebungen von Regierungen weltweit, sich durch Verpflichtungen zum Einbau von staatlichen Hintertüren in kommerzielle Kommunikationsplattformen und/oder das Hacken von informationstechnischen Systemen und

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 26. März 2018 übermittelt.*

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

Verschlüsselungssoftware in Gestalt des staatlichen Einsatzes u. a. von Spionagesoftware und „Trojanern“ Zugang zu Daten und Kommunikationen zu verschaffen, sind vor diesem Hintergrund umstritten. Staatliche Maßnahmen wie beispielsweise das bewusste Offenhalten und Ausnutzen von Schwachstellen und Sicherheitslücken schwächen IT-Systeme oft dergestalt, dass die Integrität digitaler Infrastrukturen und Produkte insgesamt geschwächt und auch unbefugte Dritte missbräuchlich davon Nutzen ziehen können. Eine kohärente Position der Bundesregierung in Bezug auf den Umgang mit Verschlüsselungstechnologien ist aus Sicht der Fragesteller bis heute nicht erkennbar. So formuliert die Bundesregierung in ihrer „Digitalen Agenda 2014 – 2017“ einerseits das Ziel, „Verschlüsselungsland Nummer eins auf der Welt“ zu werden, schafft andererseits aber mit ZITiS – Zentrale Stelle für Informationstechnik im Sicherheitsbereich eine Behörde, die darauf abzielt, Schwachstellen auszumachen und Kryptografie zu brechen.

Die Zulassung staatlichen Hackings verschiebt das Interesse zumindest der Sicherheitsbehörden auch auf die systematische Geheimhaltung, Offenhaltung und Nutzung von Schwachstellen und Sicherheitslücken in IT-Systemen, Hard- und Software. Besonders brisant erscheint, dass für das Aufspielen von Spionagesoftware auf Zielrechner oftmals nicht allein kriminalistische List, sondern erst der staatliche Ankauf von Schwarzmarktinformationen über bislang unerkannte Sicherheitslücken ausreicht (vgl. u. a. dazu www.kas.de/wf/doc/kas_51506-544-1-30.pdf?180209124944). Durch die Zusammenarbeit mit Privatfirmen wird der Schwarzmarkt für Sicherheitslücken zudem zumindest indirekt weiter befeuert.

Das Bundesverfassungsgericht nahm den Konflikt um staatliches Hacking zum Anlass, die Grundrechtsdogmatik weiterzuentwickeln und das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Artikel 2 Absatz 1 des Grundgesetzes (GG) herauszuarbeiten. Umstritten bleibt, ob und in welchem Umfang die Anforderungen des Gerichts für einen rechtsstaatlich vertretbaren Einsatz von Spionagesoftware rechtlich wie tatsächlich überhaupt umgesetzt werden können. Vorherige Versionen des sogenannten Staatstrojaners haben sich nach einer Analyse des Quellcodes durch den Chaos Computer Club e. V. als mit rechtlichen Vorgaben nicht vereinbar erwiesen. Bemühungen der Sicherheitsbehörden, geeignetes Personal zu finden und eigene Überwachungsprogramme zu entwickeln, haben nicht zum erwünschten Erfolg geführt, so dass heute erneut auf Programme von Privatfirmen zurückgegriffen wird (www.heise.de/newsticker/meldung/BKA-will-maechtigeren-Staatstrojaner-angeblich-noch-2017-einsatzbereit-haben-3779770.html). Dies ist insofern fragwürdig, als dass einzelnen Anbietern nachgewiesen werden konnte, dass – auch durch öffentliche Mittel – programmierte Programme, später mit Hilfe einer sogenannten Nachladefunktion um zusätzliche Funktionen erweitert, in autoritäre Staaten exportiert wurden und dort zu Menschenrechtsverletzungen beigetragen haben (www.heise.de/newsticker/meldung/Generalbundesanwalt-nimmt-Einsatz-von-Ueberwachungssoftware-FinFisher-ins-Visier-2551400.html). Die Verfassungskonformität dieser Programme steht zumindest in Zweifel. Eine (Quellcode-)Überprüfung durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat nach Kenntnis der Fragesteller bis heute nicht stattgefunden.

Die Beantwortung der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN (Bundestagsdrucksache 18/13413) und der Fraktion DIE LINKE. (Bundestagsdrucksache 19/522), wonach inzwischen die auch und gerade unter autoritären Staaten beliebte (vgl. www.heise.de/newsticker/meldung/Generalbundesanwalt-nimmt-Einsatz-von-Ueberwachungssoftware-FinFisher-ins-Visier-2551400.html) kommerzielle Hacking-Software Gamma/FinFisher/FinSpy vom Bundesminister des Innern zum Einsatz durch das Bundeskriminalamt (BKA) freigegeben sei, geben dringenden Anlass zu weiterer parlamentarischer Befassung.

Der TeleTrusT – Bundesverband IT-Sicherheit e. V., dem auch das BKA und das Bundesamt für Sicherheit in der Informationstechnik (BSI) angehören, wird gegen die neu geschaffenen Rechtsgrundlagen zur Onlinedurchsuchung/Quellen-Telekommunikationsüberwachung Verfassungsbeschwerde erheben (vgl. www.golem.de/news/teletrust-it-sicherheitsverband-will-gegen-staatstrojaner-klagen-1708-129395.html).

## Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 4, 5, 6, 9, 20, 22, 23 und 25 in offener Form ganz oder teilweise nicht erfolgen kann. Die in diesen Fragen erbetenen Auskünfte sind 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. Deshalb sind einzelne Informationen gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Bezüglich der in den Fragen 12 und 13 erbetenen Informationen zu Namen von Unternehmen, mit denen die Sicherheits- und Strafverfolgungsbehörden in Kontakt stehen, ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Fragen nicht – auch nicht in eingestufter Form – beantwortet werden können. Gegenstand der Fragen 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 Verfassungsrang genießende schutzwürdige Interessen des Staatswohls begrenzt.

Eine Bekanntgabe von Unternehmen, die mit den Sicherheits- und Strafverfolgungsbehörden kooperieren, würde zum Einen weitgehende Rückschlüsse auf die technischen Fähigkeiten und die Arbeitsweise zulassen und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential der Sicherheits- und Strafverfolgungsbehörden schließen lassen. Zudem würde eine Bekanntgabe von Namen jegliches Vertrauen in eine Zusammenarbeit negativ beeinflussen oder sogar zum Abbruch von Geschäftsbeziehungen führen. Dadurch würden die technischen Möglichkeiten der Behörden negativ beeinflusst und der Erfolg zukünftiger Maßnahmen konterkariert werden. Dies hätte zur Folge, dass die Fähigkeiten, mit nachrichtendienstlichen bzw. verdeckten kriminalpolizeilichen Mitteln Informationen zu gewinnen, in erheblicher Weise negativ beeinflusst werden und die Sicherheits- und Strafverfolgungsbehörden bei der Wahrnehmung ihrer Aufgaben von wesentlichen Erkenntnisquellen ausgeschlossen würden.

* Das Bundesministerium des Innern, für Bau und Heimat hat die Antworten zu den Fragen 4 bis 6, 9, 20, 22, 23 und 25 als „VS – Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Die Gewinnung solcher Informationen ist für die Sicherheit der Bundesrepublik Deutschland jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage in Deutschland drohen.

Bezüglich der in den Fragen 14, 15, 21, 36, 37 sowie Frage 44 erbetenen Informationen stehen überwiegende Belange des Geheimschutzes einer Beantwortung entgegen. Mit Auskünften zu den zur Verfügung stehenden kriminaltaktischen und nachrichtendienstlichen Vorgehensweisen und damit zu konkreten Strategien und Maßnahmen würde die Bundesregierung polizeiliche und nachrichtendienstliche Vorgehensweisen zur Verhinderung und Aufklärung von Straftaten offenlegen oder Rückschlüsse darauf ermöglichen und damit die Arbeitsfähigkeit und Aufgabenerfüllung der Sicherheits- und Strafverfolgungsbehörden gefährden, weil Täter ihr Verhalten anpassen und künftige Maßnahmen dadurch erschweren oder gar vereiteln könnten. Eine Preisgabe dieser sensiblen Informationen würde sich auf die staatliche Aufgabenwahrnehmung im Gefahrenabwehrbereich wie auch auf die Durchsetzung des Strafverfolgungsanspruchs außerordentlich nachteilig auswirken.

Daraus folgt, dass die erbetenen Informationen derartig schutzbedürftige evidente Geheimhaltungsinteressen berühren, dass auch das geringfügige Risiko eines Bekanntwerdens, wie es auch bei einer Übermittlung dieser Informationen an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In der Abwägung des parlamentarischen Informationsrechts der Abgeordneten einerseits und der staatswohlbegründeten Geheimhaltungsinteressen andererseits muss das parlamentarische Informationsrecht daher ausnahmsweise zurückstehen.

1. Hält die Bundesregierung ihre bisherige IT-Sicherheitspolitik, vor allem bezüglich des staatlichen Aufkaufs von Sicherheitslücken, für die Integrität digitaler Infrastrukturen und Angebote für förderlich?

2. Hält die Bundesregierung ihre bisherige IT-Sicherheitspolitik, vor allem hinsichtlich der eigenen Positionierung zum Umgang mit Verschlüsselungstechnologien, für die Integrität digitaler Infrastrukturen und Angebote für förderlich?

Die Fragen 1 und 2 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung hat sich bereits im Jahr 1999 mit dem Kabinettbeschluss „Eckpunkte der deutschen Kryptopolitik“ gegen jegliche Schwächung, Modifikation oder Verbot von Verschlüsselung oder ein Kompromittieren von Sicherheitsstandards der digitalen Kommunikation bekannt. Gleichzeitig gilt aber auch, dass durch die Verbreitung starker Verschlüsselungsverfahren die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden nicht ausgehöhlt werden dürfen. Die Bundesregierung hält deshalb ihre bisherige IT-Sicherheitspolitik, vor allem hinsichtlich der eigenen Positionierung zum Umgang mit Verschlüsselungstechnologien, für die Integrität digitaler Infrastrukturen und Angebote für förderlich.

3. Teilt die Bundesregierung die kritische Auffassung des Bundesrechnungshofs vom 5. Februar 2015 (https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/), wonach der zusätzliche Ankauf der umstrittenen kommerziellen Hacking-Software FinSpy letztlich auf technische Schwierigkeiten mit der Schaffung eines einsatzfähigen eigenen Spionagetrojaners (RCIS) zurückzuführen ist?

Nein, denn zur Durchführung von Maßnahmen der informationstechnischen Überwachung werden verschiedene Softwareprodukte genutzt, um die operativen Bedarfslagen abzudecken. Es ist deshalb erforderlich, hierfür auch unterschiedliche Softwareprodukte vorzuhalten.

4. In der Konkurrenz mit welchen Unternehmen erhielt die TÜV Informationstechnik GmbH Essen in der Auswahl den Zuschlag, und aufgrund welcher maßgebenden Kriterien (https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/)?

5. Trifft es zu, dass für die Prüfung von FinSpy auf Einhaltung der Leistungsvorgaben das Unternehmen CSC Deutschland Solutions GmbH beauftragt wurde (www.spiegel.de/netzwelt/netzpolitik/staatstrojaner-die-bundesregierung-schweigt-sich-aus-a-1190424.html), und worauf stützt sich ggf. die regierungsseitige Annahme der Vertrauenswürdigkeit dieses Unternehmens für die betraute Aufgabe?

6. Warum wurde in diesem Fall nicht ebenfalls die in der Presse erwähnte TÜV Informationstechnik Essen beauftragt (www.spiegel.de/netzwelt/netzpolitik/staatstrojaner-die-bundesregierung-schweigt-sich-aus-a-1190424.html)?

Die Fragen 4, 5 und 6 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Das BKA hat externe Prüfinstitute mit der Überprüfung von Produkten der informationstechnischen Überwachung (Quellen-Telekommunikationsüberwachung / Online-Durchsuchung) beauftragt; die entsprechenden Beschaffungen wurden auf Grundlage der aktuellen rechtlichen Vorgaben durch das Beschaffungsamt des Bundesministeriums des Innern, für Bau und Heimat durchgeführt. Im Zuge des Vergabeverfahrens haben die externen Prüfinstitute dargelegt, dass die geforderten Rahmenbedingungen eingehalten werden.

Ziel der Überprüfung der entsprechenden Produkte war die Bestätigung der Konformität mit gesetzlichen Vorgaben. Im Übrigen wird auf die Vorbemerkung der Bundesregierung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

7. Was bedeutet die Bescheinigung der Einhaltung von IT-Standards (z. B. Common Criteria) in Bezug auf die BKA-Spionagesoftware RCIS konkret?

Der Begriff „Spionagesoftware“ ist für Software zur Durchführung von Maßnahmen der informationstechnischen Überwachung, die durch die Strafverfolgungs- und Ermittlungsbehörden des Bundes rechtmäßig auf der Grundlage der einschlägigen gesetzlichen Befugnisnormen eingesetzt wird, nicht zutreffend.

Die Einhaltung von IT-Standards dient bei Software zur Durchführung von Maßnahmen der informationstechnischen Überwachung vor allem dem Schutz der übertragenen Daten. Hierdurch werden die Authentizität, Vertraulichkeit und Integrität der zu übertragenen Daten sichergestellt.

8. Wurde eine vollständige Quellcode-Überprüfung von FinSpy durchgeführt, und wenn ja, durch welche Stelle, und mit welchem Ergebnis?

9. Wurden Penetrationstests der Software FinSpy durchgeführt, und wenn ja, durch welche Stelle, und mit welchem Ergebnis?

Die Fragen 8 und 9 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die im Portfolio des BKA befindlichen Produkte zur Durchführung von Maßnahmen der informationstechnischen Überwachung werden vor ihrem Einsatz auf Konformität mit der aktuellen Rechtslage geprüft. Erst nach positivem Abschluss dieser Prüfungen werden die Produkte für den Einsatz freigegeben.

Bezüglich Frage 9 wird darüber hinaus auf die Vorbemerkung der Bundesregierung und den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

10. Ist die Bundesregierung der Ansicht, dass die derzeit durch Bundes- oder Landesbehörden eingesetzten IT-Überwachungs- oder Spionageprogramme einer erneuten Überprüfung hinsichtlich ihrer Verfassungskonformität Stand halten?

Zu der unzutreffenden Bezeichnung „Spionageprogramme“ wird auf die Antwort zu Frage 7 verwiesen.

Die Bundesregierung kann diese Frage nur für den eigenen Zuständigkeitsbereich, also für die Strafverfolgungs- und Sicherheitsbehörden des Bundes, beantworten. Die Bundesregierung sieht keinen Anlass, die Verfassungskonformität des Einsatzes der in der Frage erwähnten Technologie in Zweifel zu ziehen.

11. Hält die Bundesregierung die Zusammenarbeit mit Privatfirmen in diesem verfassungsrechtlich heiklen Bereich im Allgemeinen und mit den erwähnten Firmen im Speziellen für gänzlich unproblematisch, oder welche Herausforderungen ergeben sich hier aus Sicht der Bundesregierung?

Die Privatwirtschaft bietet Dienstleistungen und Produkte an, auf die die Bundesregierung zugreift, wenn sie keine eigenen Fähigkeiten bereitstellen kann und die kommerziell verfügbaren Produkte oder Dienstleistungen zur Erfüllung ihrer gesetzlichen Aufgaben geeignet sind. Gerade im Hochtechnologiebereich ist eine Zusammenarbeit mit Privatfirmen unerlässlich.

Die Zusammenarbeit erfolgt unter definierten Rahmenbedingungen (z. B. Geheimschutzbetreuung, Datenschutz, Qualitätssicherung, Auflagen).

12. Welche Unternehmen haben die Bundesregierung und/oder ihr nachgeordnete Behörden bezüglich des Ankaufs von Wissen um Softwaresicherheitslücken (Exploits) kontaktiert (bitte um Auflistung der Firmen und Daten der Kontaktaufnahme)?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

13. Gab es diesbezüglich bereits Treffen mit Unternehmensvertretern (bitte um Auflistung der Unternehmen, Ort und Daten der Treffen)?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

14. Haben die Bundesregierung und/oder ihr nachgeordnete Behörden bereits das Wissen um Sicherheitslücken von kommerziellen oder nichtkommerziellen Anbietern erworben (bitte um Auflistung von wem, wann, und wie hoch waren die Kosten)?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

15. Welche Maßnahmen hat die Bundesregierung unternommen, um sicherzustellen, dass entsprechende Programme, sowohl im unveränderten wie im modifizierten Zustand, nicht an Dritte weiterverkauft werden, z. B. durch entsprechende Vertragsvereinbarungen?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

16. Welche Maßnahmen hat die Bundesregierung unternommen, um sicherzustellen, dass eine regelmäßige Quellcodeprüfung der im Einsatz befindlichen Programme vor allem hinsichtlich einer Überprüfung der Verfassungskonformität möglich ist, z. B. durch entsprechende Vertragsvereinbarungen?

Produkte zur Durchführung von Maßnahmen der informationstechnischen Überwachung werden vor ihrem Einsatz auf Konformität mit der aktuellen Rechtslage geprüft und fortlaufend weiterentwickelt.

17. Bedeutet die Bereitstellung des sog. Protokollierungssystems ProSys, dass mit Hilfe dieser Software eine vollständige Revisionsfähigkeit von Einsätzen der den Sicherheitsbehörden zur Verfügung stehenden Spionageprogramme erzielt werden kann?

18. Auf welche Weise werden mittels des Protokollierungssystems ProSys welche Daten des Trojanereinsatzes protokolliert?

19. Welche Kosten sind durch die BKA-Entwicklung des Protokollierungssystems ProSys bis heute angefallen?

20. Ist die Weiterentwicklung der Protokollierungssoftware ProSys für den Einsatz in den Ländern bereits erfolgt, und wurde sie Sicherheitsbehörden der Länder bereits zur Verfügung gestellt?

    Wenn ja, welchen?

Die Fragen 17 bis 20 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Hinsichtlich Frage 18 ist zunächst darauf hinzuweisen, dass seitens der Strafverfolgungsbehörden des Bundes keine „Trojaner“ eingesetzt werden. Als „Trojaner“ werden in der Regel Schadprogramme bezeichnet, die widerrechtlich auf informationstechnischen Systemen ausgeführt werden und ohne Wissen des Anwenders eine andere Funktion erfüllen. Der Begriff „Trojaner“ ist folglich für Software zur Durchführung von Maßnahmen der informationstechnischen Überwachung, die durch die Strafverfolgungsbehörden des Bundes rechtmäßig auf der Grundlage der einschlägigen gesetzlichen Befugnisnormen eingesetzt wird, nicht zutreffend.

Das Protokollierungssystem ProSys ist Bestandteil der vom BKA entwickelten Software RCIS (zusammenhängendes Produkt). Die Protokollierung von Maßnahmen der informationstechnischen Überwachung erfolgt auf Grundlage der aktuellen Rechtslage. Eine Erhebung der davon auf die Teilkomponente „ProSys“ der Quellen-TKÜ-Software „RCIS“ angefallenen Ausgaben erfolgt nicht.

Bezüglich Frage 20 wird darüber hinaus auf die Vorbemerkung der Bundesregierung und den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

21. Trifft es, wie in der Presse berichtet (www.welt.de/politik/deutschland/article 173121473/Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html) zu, dass die BKA-Eigenentwicklung RCIS bis heute keine Zugriffe auf Betriebssysteme mobiler Endgeräte wie Smartphones ermöglicht?

Die vom BKA entwickelte Quellen-TKÜ-Software „RCIS“ wird in Abhängigkeit von der operativen Bedarfslage kontinuierlich weiterentwickelt. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

22. Welche Kosten sind durch die BKA-Eigenentwicklung der Spionagesoftware RCIS bis heute angefallen?

Es wird auf den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

23. In wie vielen Fällen ist RCIS seit der Betriebsbereitschaft und der Einsatzfreigabe bislang je unter welcher Befugnisnorm zum Einsatz gekommen?

Es wird auf die Vorbemerkung der Bundesregierung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

24. In wie vielen dieser Fälle wurde der Einsatz aufgrund welcher Kriterien intern als erfolgreich im Sinne der Aufgabenstellung bewertet?

Es wird auf die Antwort zu Frage 23 verwiesen.

25. Wie viele sog. Zero-Day-Sicherheitslücken sind den Bundesbehörden zwischenzeitlich (zumindest seit der Antwort auf die letzte Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN vom 13. September 2017 auf Bundestagsdrucksache 18/13413) bekannt und werden vor der Öffentlichkeit geheim gehalten?

a) Wie lange werden diese bereits zurückgehalten, bzw. sind diese den einschlägigen Meldepflichten staatlicher Stellen bereits entzogen?

b) Auf der Basis welcher Rechtsgrundlage bzw. welchen Verfahrens wird die Entscheidung darüber getroffen, ob und für welche Dauer eine IT-Sicherheitslücke für die Nutzung zu eigenen Zwecken von der Meldung zurückgehalten wird?

c) Wer übernimmt nach Auffassung der Bundesregierung die maßgebende Verantwortung dafür, welche Informationen über Schwachstellen die Sicherheitsbehörden für sich behalten und welche sie dem Hersteller und/oder dem BSI melden, damit diese zum Schutz der Allgemeinheit behoben werden können?

d) Liegen bislang überhaupt Vorgaben für ein derartiges rechtsstaatliches Verfahren u. a. zur Vornahme einer Bewertung der Risiken für die Allgemeinheit vor, und wenn nein, warum nicht?

e) Wird das BSI in jedem Falle in einen derartigen Entscheidungsprozess einbezogen, und wenn nein, warum nicht?

f) Wie viele dem sog. Telegram-Fall (https://netzpolitik.org/2016/bundeskriminalamt-knackt-telegram-accounts/) vergleichbare Verfahren der gezielten Ausnutzung einer Schwachstelle eines gängigen IT-Systems und/oder Messengerprodukts sind den Sicherheitsbehörden noch bekannt und werden von diesen intern für die Infiltration im Rahmen bereits bestehender, allgemeiner Eingriffsnormen ebenfalls für zulässig erachtet?

g) Wie oft wurden diese weiteren Verfahren der Ausnutzung von Schwachstellen bislang im Rahmen welcher Verfahren durch Bundesbehörden eingesetzt (bitte einschlägige Rechtsgrundlage angeben)?

h) Teilt die Bundesregierung die Auffassung, dass auch die Entscheidung über die Nutzung dieser Schwachstellen und die damit einhergehende Nichtmeldung an das BSI und/oder die Öffentlichkeit zumindest einem rechtsstaatlichen Verfahren und ggf. einer hinreichend bestimmten, bereichsspezifischen rechtlichen Regelung unterliegen sollte, und wenn nein, warum nicht?

i) Besteht zumindest auf Seite der Bundesregierung Transparenz hinsichtlich der verschiedenen, im Einsatz befindlichen oder in der Entwicklung befindlichen Verfahren zur gezielten staatlichen Ausnutzung von IT-Schwachstellen durch bundesdeutsche Sicherheitsbehörden, um ein insoweit umfassenderes Lagebild der Risikosteigerung für die IT-Sicherheit erhalten zu können, und wenn ja, wie erreicht die Bundesregierung diesen Überblick derzeit?

j) Bedarf es aus Sicht der Bundesregierung, auch unabhängig von der Frage rechtlicher Zulässigkeit des bisherigen Vorgehens, deshalb zumindest eines internen IT-Schwachstellenmanagements (Beschaffung, Bewertung und Abwägung, Verwendung und Sicherung), um z. B. doppelte Ankäufe von Zero Day Exploits auf den illegalen Märkten zu verhindern?

k) Worin bestehen nach Ansicht der Bundesregierung derzeit die verbindlichen ethischen wie rechtsstaatlichen Rahmenbedingungen für die Beschaffung von Sicherheitslücken, um die staatliche Förderung eines illegalen Marktes zu verhindern, auf dem auch autoritäre Staaten ihre Software zur Überwachung von Zivilgesellschaft und politischen Gegnern sowie Straftäter ihre Instrumente beziehen (vgl. dazu Herpig/Schmitz, www.security-insider.de/oeffentliche-sicherheit-kontra-it-sicherheit-a-658471/)?

l) Welche internationalen Gremien und Stellen sind nach Auffassung der Bundesregierung zu beteiligen, wenn durch diese bislang nicht veröffentlichte ZeroDays zum Einsatz kommen?

Es wird auf die Vorbemerkung der Bundesregierung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil verwiesen.

26. Wurden bereits oder werden derzeit bereits entsprechend den Vorgaben des Entwurfs des aktuellen Koalitionsvertrages zwischen CDU, CSU und SPD seitens der Bundesministerien der geschäftsführenden Bundesregierung Vorbereitungen für die Schaffung weiterer Rechtsgrundlagen für den Einsatz von Trojanerspionagesoftware durch das Bundesamt für Verfassungsschutz (BfV) sowie den Bundesnachrichtendienst (BND) getroffen, und wenn ja, welche?

27. Welche weiteren „rechtlichen, organisatorischen sowie technischen Rahmenbedingungen“ plant die Bundesregierung entsprechend den Vorgaben des Entwurfs des Koalitionsvertrages zu schaffen, um „die Sicherheitsbehörden bei der Verfolgung und Prävention von Cyberkriminalität zu stärken“ (vgl. Entwurf des Koalitionsvertrages zwischen CDU, CSU und SPD)?

Die Fragen 26 und 27 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Hinsichtlich des unzutreffenden und der Bundesregierung überdies unbekannten Begriffs „Trojanerspionagesoftware“ wird auf die Antworten zu Fragen 7 und 18 verwiesen.

Es bleibt der neuen Bundesregierung vorbehalten, über das Nähere der Umsetzung des Koalitionsvertrags zu entscheiden. Aus dem Grundsatz der Gewaltenteilung folgt ein Kernbereich exekutiver Eigenverantwortung, der einen auch parlamentarisch grundsätzlich nicht ausforschbaren Initiativ-, Beratungs- und Handlungsbereich einschließt. Dazu gehört die Willensbildung der Regierung selbst, sowohl hinsichtlich der Erörterungen im Kabinett als auch bei der Vorbereitung von Kabinett- und Ressortentscheidungen, die sich vornehmlich in ressortübergreifenden und -internen Abstimmungsprozessen vollzieht.

Eine Pflicht der Regierung, parlamentarischen Informationswünschen zu entsprechen, besteht danach in der Regel nicht, wenn die Information zu einem Mitregieren Dritter bei Entscheidungen führen kann, die in der alleinigen Kompetenz der Regierung liegen (BVerfGE 124, 78 [125]; 137, 185 [234]).

Die Kontrollkompetenz des Parlaments erstreckt sich daher grundsätzlich nur auf bereits abgeschlossene Vorgänge und umfasst nicht die Befugnis, in laufende Verhandlungen und Entscheidungsvorbereitungen einzugreifen (BVerfGE 124, 78 [120 f.]). Die interne Willensbildung in der Bundesregierung zu „rechtlichen, organisatorischen sowie technischen Rahmenbedingungen“, um „die Sicherheitsbehörden bei der Verfolgung und Prävention von Cyberkriminalität zu stärken“, ist noch nicht abgeschlossen.

28. Welche Position vertritt die Bundesregierung gegenwärtig im Rahmen von Diskussionsprozessen von EU-Institutionen in Bezug auf die weiterhin vernehmbare Forderung nach staatlichen Verpflichtungen von IT-Unternehmen zur Bereitstellung von Hintertüren zur Ermöglichung verdeckter Zugriffe von Sicherheitsbehörden (sog. Backdoors)?

Im Rahmen von Diskussionsprozessen von EU-Institutionen spricht sich die Bundesregierung stets gegen die Implementierung von Hintertüren oder die Schwächung von Verschlüsselungsstandards aus.

Ergänzend wird auf die Antwort zu Frage 2 verwiesen.

a) Wurden oder werden die Spionagetrojaner von Bundesbehörden bereits in ihrer Funktion als sog. Keylogger eingesetzt?

Hinsichtlich des unzutreffenden und der Bundesregierung überdies unbekannten Begriffs „Spionagetrojaner“ wird auf die Antworten zu den Fragen 7 und 18 verwiesen. Der Einsatz der Funktionen bei Maßnahmen der informationstechnischen Überwachung erfolgt nach strengen verfassungsrechtlichen Rahmenbedingungen und Vorgaben.

b) Wenn ja, kann der Einsatz für diesen Zweck nachweislich auf diese Funktion beschränkt werden?

Es wird auf die Antwort zu Frage 28a verwiesen.

Nach der Rechtsprechung des Bundesverfassungsgerichts können Keylogger auf der Grundlage der für die Online-Durchsuchung jeweils einschlägigen Rechtsgrundlagen eingesetzt werden. Einer zwingenden Beschränkung allein auf diese Funktion bedarf es im Rahmen einer Online-Durchsuchung indes nicht, der Umfang der Online-Durchsuchung bemisst sich vielmehr nach der im konkreten Einzelfall geprüften Erforderlichkeit.

c) Welche Rechtsgrundlage steht nach Auffassung der Bundesregierung für diese Form des Einsatzes zur Verfügung?

Es wird auf die Antwort zu Frage 28a verwiesen.

29. Kommt es im Rahmen des Einsatzes von FinFisher zu einer – wenn auch nur vorübergehenden – Speicherung personenbezogener Daten auf Servern des Betreiberunternehmens?

Die Speicherung personenbezogener Daten im Rahmen der vom BKA durchgeführten Maßnahmen der informationstechnischen Überwachung erfolgt ausschließlich auf IT-Systemen, die dem Administrationsbereich des BKA unterliegen.

30. Erfolgte bislang eine datenschutzrechtliche Kontrolle auch des kommerziellen Spionagetrojaners FinSpy durch die BfDI, und wenn ja, mit welchem Ergebnis?

31. Hat die Bundesregierung der BfDI vollumfänglich alle von ihr zur datenschutzrechtlichen Prüfung gemäß dem Bundesdatenschutzgesetz angeforderten Unterlagen, Daten und Informationen zu beiden Vorgängen (RCIS und FinSpy) vorgelegt, und wenn nein, warum nicht?

32. Liegt zwischenzeitlich ein abschließender Prüfbericht der BfDI zur eigenentwickelten Spionagesoftware des BKA vor, und wenn ja, mit welchem Ergebnis?

Die Fragen 30 bis 32 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat im Juni 2016 im Rahmen der gesetzlich zugewiesenen Aufgaben einen Kontrollbesuch beim BKA durchgeführt; es wurden Produkte für die informationstechnische Überwachung geprüft.

Der BfDI wurden zum Zwecke der Prüfung alle angeforderten Informationen zur Verfügung gestellt. Das Ergebnis des Kontrollbesuchs wurde durch die BfDI in geeigneter Form dokumentiert.

33. Wurde bei den bislang zum Einsatz gekommenen Nutzungen von IT-Schwachstellen von Zielsystemen jeweils in Absprache oder zumindest Inkenntnissetzung oder informell mit dem BSI gehandelt?

Die Behörde, die Kenntnis von einer Schwachstelle erhält, koordiniert und konsolidiert die Informationsweitergabe.

34. Welche konkreten Verbesserungen der technischen Möglichkeiten der Sicherheitsbehörden zur Entschlüsselung verschlüsselter Datenträger kann die neu geschaffene Arbeitseinheit ZITiS bereits vorweisen (bitte nach Dienstleistungen für Bundeswehr, Kommando Cyberraum, BKA, Verfassungsschutz/BfV, andere aufschlüsseln)?

ZITiS befindet sich derzeit im Aufbau. Ergebnisse im Sinne der Fragestellung liegen noch nicht vor.

a) Wie viele Fachleute stehen der ZITiS für die ihr zugedachten operativen Aufgaben inzwischen tatsächlich zur Verfügung?

Der ZITIS stehen insgesamt 34 Personen (Stand: 1. März 2018) für den Aufbau und zur Aufgabenerfüllung zur Verfügung.

b) Ist es dafür bislang zu Personalwechseln aus anderen, mit der Entwicklung von IT-Angriffen befassten Arbeitseinheiten (etwa des Kompetenzzentrums Informationstechnische Überwachung des BKA, Referaten des Bundesministeriums des Innern, des BND usw.) gekommen?

Wenn ja, welchen genau?

Nein.

c) Ist die Bundesregierung auch weiterhin der Ansicht, dass es keiner Rechtsgrundlage für ZITiS bedarf?

ZITiS ist per Erlass des BMI im April 2017 errichtet worden. Dieser Erlass stellt eine rechtliche Grundlage für Errichtung der ZITiS dar (Gemeinsames Ministerialblatt (GMBI) vom 20. April 2017, S. 274).

Die Bundesregierung ist auch weiterhin der Ansicht, dass es keiner weiteren Rechtsgrundlage für ZITIS bedarf.

35. In wie vielen Fällen wurde nach Kenntnis der Bundesregierung bereits Software des israelischen Sicherheitsunternehmens Cellebrite (z. B. UFED) zur Extraktion von Daten in Strafverfahren und/oder polizeilichen Verfahren eingesetzt (bitte getrennt anführen)?

Grundsätzlich werden forensische Softwareprodukte u. a. von Cellebrite zum Auslesen von sichergestellten bzw. beschlagnahmten Mobilfunkendgeräten gemäß den gesetzlichen Grundlagen verwendet. Eine Aufschlüsselung oder statistische Erfassung hinsichtlich der Nutzung der extrahierten Daten nach Verfahrensarten erfolgt nicht.

a) In wie vielen Fällen wurde Software des israelischen Sicherheitsunternehmens Cellebrite (z. B. UFED) zur Extraktion von Daten nach § 15a des Asylgesetzes eingesetzt?

Die Software der Firma Cellebrite wurde in keinem Fall zur Extraktion von Daten nach § 15a des Asylgesetzes (AsylG) eingesetzt.

b) Welche Kosten sind hierbei jeweils und insgesamt angefallen?

Auf die Antwort zu Frage 35a wird verwiesen. Im Übrigen erfolgt keine Aufschlüsselung hinsichtlich der Nutzung der extrahierten Daten nach Verfahrensarten.

c) Auf welcher datenschutzrechtlichen und sonstigen vertraglichen Basis kommen nach Kenntnis der Bundesregierung Produkte dieses Unternehmens in bundesdeutschen hoheitlichen Verfahren zum Einsatz?

Die eingesetzten Produkte von Cellebrite kommen bei bundesdeutschen hoheitlichen Verfahren ausschließlich nach Vorgabe der gesetzlichen Rahmenbedingungen zum Einsatz. Werkzeuge (Hard- und Software) für die digitale Forensik werden in eigenen internen Netzwerken betrieben. Datenschutzrechtliche Belange werden nach den gesetzlichen Vorgaben berücksichtigt.

d) Wurden nach Kenntnis der Bundesregierung bereits oder werden inzwischen FinFisher/RCIS vergleichbare Überprüfungen der Funktionalität und der Datensicherheit der zum Einsatz kommenden Cellebrite-Software durchgeführt (etwa Quellcode-Prüfungen), um z. B. den Abfluss von Daten aus Verfahren bundesdeutscher Behörden an unbefugte dritte Stellen (z. B. Drittstaaten) ausschließen zu können, und wenn ja, mit welchem Ergebnis?

Es wurden keine Quellcode-Prüfungen durchgeführt. Ein Abfluss von Daten im Rahmen von IT-forensischer Untersuchung an unbefugte Stellen ist nicht möglich, da in diesem Rahmen keine Daten in mit dem Internet verbundenen Netzen oder beim Hersteller gespeichert werden.

e) Führt die Verwendung der Cellebrite-Software zur – wenn auch nur vorübergehenden – Speicherung von personenbeziehbaren Daten auf Servern des Unternehmens Cellebrite selbst?

Der Einsatz von Produkten der Fa. Cellebrite führt in keinem Fall zu Speicherungen von personenbeziehbaren Daten beim Hersteller. Auf die Antwort zu Frage 35d wird verwiesen.

36. Welche Vorgehensweisen der kriminalistischen List unterscheidet die Bundesregierung, mit denen auf rechtlich de lege lata noch zulässige Weise ein Aufbringen der Spionagesoftware auf Zielrechner erfolgen kann (bitte im Einzelnen darlegen)?

37. Welche dieser Vorgehensweisen haben Bundesbehörden bislang in jeweils welchem Umfang eingesetzt (etwa durch verdeckte Maßnahmen an Rechnern in der Wohnung von Tatverdächtigen, bei unbeobachteten Maßnahmen im Rahmen von Zollkontrollen oder Personenkontrollen, durch staatlichen Phishing-Einsatz per E-Mail; durch Drive-By-Infektionen auf manipulierten Webseiten usw.)?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

38. Welche Anstrengungen hat die Bundesregierung unternommen, um eine wissenschaftlich verlässliche und valide Datenbasis zur Bewertung zu erhalten, in wie vielen Fällen Ermittlungen oder Verfahren eingestellt werden mussten, weil Zielrechner/Smartphones usw. aufgrund von Verschlüsselung nicht überwacht werden konnten?

Im Sinne einer wissenschaftlich verlässlichen und validen Datenbasis werden Erhebungen von der Bundesregierung bislang nicht vorgenommen; beim BKA existiert jedoch, um bei polizeilich erkannten gesetzlichen Defiziten für die polizeiliche Aufgabenwahrnehmung einen gesetzgeberischen Handlungsbedarf anhand von Praxisfällen aufzuzeigen, eine „Rechtstatsachensammel- und -auswertestelle“ (RETASAST).

Eine für den Zeitraum 2012 bis 2013 (292 Fälle) durchgeführte Erhebung durch die RETASAST ergab, dass der Einsatz von Kryptierungsdiensten in 72 Prozent der Verfahren belegt werden konnte. Darüber hinaus führte die Erhebung zum Ergebnis, dass in 67 Prozent der Verfahren Tatverdächtige bewusst auf die Nutzung von Kryptierungsmöglichkeiten zurückgegriffen haben.

39. Falls die Bundesregierung über eine solche Datenbasis verfügt, wie lautet das Ergebnis zu der in Frage 38 genannten Bewertung?

Die in Frage 38 erwähnte Erhebung belegt als qualitative Stichprobe das Vorhandensein von verschlüsselter Kommunikation in der überwiegenden Mehrzahl der gemeldeten Strafverfahren und damit das Problem der faktisch scheiternden Auswertung von Telekommunikationsinhalten und damit der Verlust von Ermittlungsansätzen bzw. Beweismitteln für die Strafverfolgungsbehörden.

Weitergehende Rückschlüsse auf Ablauf und Ausgang von Strafverfahren sind auf dieser Grundlage nicht möglich.

40. Welche grundrechtsschonenderen Alternativen zur rechtsstaatlich fragwürdigen Schwächung starker Verschlüsselung beforscht und prüft die Bundesregierung in welchem Umfang derzeit konkret (bitte im Einzelnen anführen), bzw. welche weiteren politischen wie operativen Vorschläge bietet sie an, um die Aufgabenverfolgung der Sicherheitsbehörden unter gleichzeitiger Wahrung der Selbstschutzmöglichkeiten von Kryptographie und Verschlüsselung zu ermöglichen?

Eine Schwächung starker Verschlüsselung wird von der Bundesregierung nicht verfolgt. Ergänzend wird auf die Antwort zu Frage 2 verwiesen.

41. Hält die Bundesregierung es für rechtlich tragfähig, angesichts der Komplexität und des Umfangs der gegebenen Weltverhältnisse, den geheimdienstlichen Einsatz technischer Aufklärung mit dem Argument zu rechtfertigen, ein vollständiges Lagebild sei ansonsten (auf herkömmlichem Wege) nicht zu erreichen (vgl. Vorbemerkung, S. 2 unten der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE., Bundestagsdrucksache 19/522), und wie definiert die Bundesregierung das Leitbild vom „vollständigen Lagebild“?

Die Bundesregierung ist darauf angewiesen, ihre Entscheidungen aufgrund vorliegender Fakten und fachlich fundierter Einschätzungen zu treffen. Nachrichtendienstliche Informationen können ein derartiges Lagebild ergänzen oder sogar maßgeblich bestimmen.

42. Wie viele internationale Partnerbehörden haben in der Vergangenheit nach der Nennung von Kontaktinformationen in der Öffentlichkeit durch die Bundesregierung ihre Zusammenarbeit mit dem BKA eingestellt, und für welche Dauer erfolgte die Einstellung der Zusammenarbeit (vgl. Vorbemerkung der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/522, S. 4)?

Im Rahmen internationaler Kooperationen und Kontakte tauscht sich das BKA regelmäßig mit ausländischen Behörden zu Maßnahmen der informationstechnischen Überwachung aus.

Dieser Austausch ist vor dem Hintergrund der globalen Herausforderungen bei der informationstechnischen Überwachung zielführend und sinnvoll. In einer einstelligen Anzahl haben internationale Partner in der Vergangenheit die Zusammenarbeit mit dem BKA nach Veröffentlichung entsprechender Kontaktinformationen in verschiedenen Ausprägungen merklich zurückgefahren und damit faktisch eingestellt. Der international notwendige Austausch auf diesem Themengebiet konnte damit nicht bzw. nur noch in sehr geringem Maße durchgeführt werden.

43. Führte das BfV in der Vergangenheit Onlinedurchsuchungen durch, und wenn ja, wie häufig, auf welcher Rechtsgrundlage, und mit welchen Softwareprodukten?

Das Bundesamt für Verfassungsschutz (BfV) hat bislang mangels Rechtsgrundlage keine Maßnahmen der Onlinedurchsuchung durchgeführt.

44. Führte der BND in der Vergangenheit und bis heute Quellen-Telekommunikationsüberwachungen sowie Onlinedurchsuchungen durch, und wenn ja, wie häufig, und mit welchen Softwareprodukten?

Unter Bezugnahme auf die Vorbemerkung der Bundesregierung kann hierzu keine Aussage getroffen werden.

45. Welche Rechtsgrundlagen standen/stehen dem BND nach Auffassung der Bundesregierung derzeit und in der Vergangenheit zur Verfügung, um Quellen-Telekommunikationsüberwachungen und/oder Onlinedurchsuchungen durchzuführen?

Maßnahmen der Quellen-Telekommunikationsüberwachungen und/oder der Online-Durchsuchungen durch den Bundesnachrichtendienst würden ggf. auf § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) gestützt werden.

46. Teilt die Bundesregierung die Auffassung der französischen Regierung, dargelegt in der „Revue stratégique de cyberdéfense“ vom 12. Februar 2018 (www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf), dass es eines internationalen Verbotes von offensiven digitalen Reaktionen auf Hackerangriffe (Hack Back) durch Private bedarf, und wird sie sich dafür einsetzen?

Die Positionierung der Bundesregierung zu diesem Punkt ist noch nicht abgeschlossen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, 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