Deutscher Bundestag **Drucksache 19/982**

19. Wahlperiode 22.02.2018

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Canan Bayram, Dr. Anna Christmann, Kai Gehring, Erhard Grundl, Anja Hajduk, Britta Haßelmann, Dieter Janecek, Katja Keul, Sven-Christian Kindler, Monika Lazar, Irene Mihalic, Filiz Polat, Tabea Rößner, Dr. Manuela Rottmann, Stefan Schmidt, Kordula Schulz-Asche, Margit Stumpp und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Staatliches Hacking von Internetkommunikation – Transparenz rechtlicher und tatsächlicher Voraussetzungen

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 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 Sicher-

heitslücken 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).

Wir fragen die Bundesregierung:

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?
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?
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)?
7. Was bedeutet die Bescheinigung der Einhaltung von IT-Standards (z. B. Common Criteria) in Bezug auf die BKA-Spionagesoftware RCIS konkret?
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?
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?
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?
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)?
13. Gab es diesbezüglich bereits Treffen mit Unternehmensvertretern (bitte um Auflistung der Unternehmen, Ort und Daten der Treffen)?

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)?
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?
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?
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?
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?
22. Welche Kosten sind durch die BKA-Eigenentwicklung der Spionagesoftware RCIS bis heute angefallen?
23. In wie vielen Fällen ist RCIS seit der Betriebsbereitschaft und der Einsatzfreigabe bislang je unter welcher Befugnisnorm zum Einsatz gekommen?
24. In wie vielen dieser Fälle wurde der Einsatz aufgrund welcher Kriterien intern als erfolgreich im Sinne der Aufgabenstellung bewertet?
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?

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)?

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)?

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

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

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

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

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?

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?

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)?

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

c) Ist die Bundesregierung auch weiterhin der Ansicht, dass es keiner 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)?

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

b) Welche Kosten sind hierbei jeweils und insgesamt angefallen?

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

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?

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

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.)?

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?

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

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?

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“?

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)?

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

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

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?

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?

Berlin, den 20. Februar 2018

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

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