Deutscher Bundestag **Drucksache 19/25549**

19. Wahlperiode 22.12.2020

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, Margit Stumpp, Dr. Anna Christmann, Dieter Janecek, Luise Amtsberg, Canan Bayram, Britta Haßelmann, Katja Keul, Monika Lazar, Filiz Polat, Dr. Manuela Rottmann, Wolfgang Wetzel und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Die Verschlüsselungspolitik der Bundesregierung und das Engagement von ZITiS zum Brechen von Kryptografie

Hochleistungsrechner und Quantencomputing haben das Potential, die Digitalisierung aller Lebensbereiche disruptiv zu verändern.

Auch für die Vertraulichkeit von Kommunikation entstehen durch den rasanten technologischen Fortschritt und die zunehmende Verbreitung von Hochleistungsrechnern und Quantentechnologie neue Chancen, beispielsweise bezüglich der Verbesserung bestehender kryptografischer Verfahren. Gleichzeitig entstehen auch Risiken, beispielsweise durch das bewusste Brechen von Kryptografie durch Sicherheitsbehörden zur Entschlüsselung vertraulicher Kommunikation.

Vollständig abhörsichere Quantennetzwerke, vielschichtige neue Anwendungsmöglichkeiten, welche die Optimierung von Prozessen oder das hochkomplexe Analysieren von Datenbanken verändern – die zunehmende Verbreitung von Hochleistungsrechnern und Quantentechnologie erfordern absehbar die Anpassung bestehender IT-Sicherheitslösungen. Hochleistungsrechner und Quantencomputer werden zukünftig absehbar nicht nur bestehende asymmetrische Kryptografiesysteme zu brechen imstande sein, sondern stellen nach Ansicht der Fragesteller darüber hinaus auch eine Bedrohung für sämtliche bestehende Verschlüsselungstechniken dar.

Angesichts der Potentiale und Risiken ist nach Ansicht der Fragesteller eine aktive politische Begleitung der technologischen Entwicklung und Investitionen in die Förderung und Forschung im Sinne des Gemeinwohls wichtig (vgl. die Kleine Anfrage des Fraktion BÜNDNIS 90/DIE GRÜNEN „Förderung von Quantentechnologien“ auf Bundestagsdrucksache 19/24762).

Projekte mit Hochleistungsrechnern und Quantencomputern, die das Ziel verfolgen, Kryptografie flächendeckend zu brechen und somit die IT-Sicherheit nachhaltig zu schwächen, sind nach Ansicht der Fragesteller abzulehnen. Dies gilt umso mehr, wenn sie von sich der parlamentarischen Kontrolle weitgehend entziehenden Einrichtungen wie der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) auf Basis unklarer und unzureichender Rechtsgrundlagen durchgeführt werden.

Insgesamt bleibt nach Ansicht der Fragesteller die deutsche Verschlüsselungspolitik hochwidersprüchlich. Um IT-Sicherheit und technologische Souveränität zu gewährleisten und der staatlichen Schutzverantwortung für die Privatheit

von Kommunikation gerecht zu werden, ist es nach Ansicht der Fragesteller dringend geboten, statt Hochleistungsrechner und Quantentechnologie für das flächendeckende Brechen von Kryptografie einzusetzen, die Förderung gesellschaftlicher sinnvoller Quantentechnologieanwendungen und der dazu notwendigen Kompetenzen auszubauen und weitere Mittel für die Erforschung an besseren kryptografischen Verfahren zu nutzen – und damit dem Gemeinwohl und dem Grundrechtsschutz zu dienen.

Bezüglich der bisherigen Kryptopolitik der Bundesregierung, der Praxis von ZITiS, Verschlüsselungen von Daten auf Rechnern und Smartphones – auch in laufenden Verfahren – zu umgehen und verschiedenen Sicherheitsbehörden von Bund und Ländern bei der Beschaffung von Sicherheitslücken und der Erstellung sogenannter „Staatstrojaner“ zu unterstützen (vgl. „Mysterium ZITIS – Was macht eigentlich die „Hackerbehörde“?, tagesschau.de vom 28. Oktober 2020, abrufbar unter https://www.tagesschau.de/investigativ/wdr/zitis-107.html), stellen sich zahlreiche Fragen, auch und vor allem bezüglich der Rechtmäßigkeit dieser Praktiken:

1. Wie bewertet die Bundesregierung die potentiellen wie konkreten Folgen und Auswirkungen, Herausforderungen und Gefahren von Hochleistungsrechnern und Quantentechnologien für den Datenschutz und bestehende kryptografische Verfahren – auch mit Blick auf bestehende bevorratete Datenbanken z. B. in deutschen (Sicherheits-)Behörden?
2. Welche möglichen Gefahren erkennt die Bundesregierung durch Hochleistungsrechner und Quantentechnologien für die IT-Sicherheit, insbesondere mit Blick auf offensive Anwendungen wie IT-Angriffe (siehe Shor- und der Grover-Algorithmus), und mit welchen konkreten Maßnahmen fördert sie die sogenannte Krypto-Agilität?
3. Inwiefern ergreift die Bundesregierung welche konkreten Maßnahmen und Förderungen, um die Sicherheit und technologische Souveränität künftig zu gewährleisten, und welche Projekte und Maßnahmen verfolgt sie, die die europäische und internationale Zusammenarbeit im Bereich Kryptografie betreffen (bitte möglichst konkret auflisten)?
4. In welchem Umfang werden aktuell die für Quantentechnologien vorgesehen Gelder für die Forschung und Entwicklung von Post-Quanten-Kryptografie verwendet, und wie soll sich dies künftig darstellen?
5. Welche Chancen und Risiken und damit einhergehenden notwendigen regulativen Maßnahmen sieht die Bundesregierung hinsichtlich staatlicher wie privater Entwicklungen für den Bereich der Sicherheit bei der Datenkommunikation (offensive und defensive Anwendungen der IT-Sicherheitsarchitektur), und welche Vorkehrungen werden aus diesen Gründen für oder in deutschen Sicherheitsbehörden getroffen, insbesondere mit Blick auf Krypto-Agilität und den Umstieg auf neue kryptografische Infrastrukturen?
6. Wie soll nach Ansicht der Bundesregierung Kryptografie angesichts dessen, dass heutige Verschlüsselungsstandards (wie asynchrone RSA-Verschlüsselung) mit Rechenleistungen von Hochleistungsrechnern und Quantencomputern absehbar gebrochen werden wird, weiterentwickelt werden, und welche konkreten Forschungsvorhaben unterstützt die Bundesregierung hier (bitte möglichst konkret auflisten)?
7. Welche Projekte verfolgt die Bundesregierung konkret, damit sensible Kommunikation zukünftig so verschlüsselt wird, dass sie nicht mit Quantencomputern nachträglich entschlüsselt werden kann?

8. Bis wann sollte nach Ansicht der Bundesregierung in Deutschland ein breites Quantenkommunikationsnetzwerk zur abhörsicheren Kommunikation aufgebaut werden, inwiefern fördert die Bundesregierung entsprechende Bemühungen, und welche Akteure sollen zukünftig wie konkret Zugang zu dieser Technologie erhalten?
9. Inwiefern und welche Entwicklungen von quantencomputerresistenten kryptografischen Systemen werden durch staatliche Behörden entwickelt oder gefördert?
10. Welche quantencomputerresistente kryptographische Verfahren hält die Bundesregierung mit Blick auf die Standardisierung in besonderem Maße für fördernswert, und wann rechnet die Bundesregierung mit der Standardisierung solcher (vgl. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen)?
11. Inwiefern haben deutsche Sicherheitsbehörden und/oder deren behördlicher Verwaltungshelfer nach Kenntnis der Bundesregierung bereits Beta-Versionen oder Simulationen von Quantencomputern im Test oder Einsatz, wenn ja, welche, und inwiefern (bitte konkret auflisten)?
12. Welche Art Hochleistungsrechner ist derzeit bei ZITiS im Einsatz?
13. Wie ist der aktuelle Entwicklungsstand beim Quantencomputer an der Bundeswehruniversität München/CODE mit IBM und der Kooperation und Nutzung durch die ZITiS?
14. Mit und auf welche Art und Weise arbeitet ZITiS in diesem Projekt zusammen, und wer konkret hat alles Zugriff auf den Quantencomputer?
15. Wie verhält sich die Bundesregierung zu dem Sachverhalt, dass laufende Projekte mit Hochleistungsrechnern und Quantentechnologie, die das alleinige Ziel verfolgen, Kryptografie zu brechen, um Sicherheitsbehörden Zugang zu Geräten und privater Kommunikation zu ermöglichen und somit die IT-Sicherheit insgesamt zu schwächen mit dem Ziel „Sicherheit und technologische Souveränität“ zu gewährleisten, in Einklang zu bringen sind, und falls ja, wie begründet sie dies?
16. Hält die Bundesregierung ein solches Vorgehen für vereinbar mit ihrer eigenen Kryptografiepolitik, und sieht die Bundesregierung, dass es weitaus sinnvoller wäre, Hochleistungsrechner und Quantentechnologie für die Forschung an besseren kryptografischen Verfahren zu nutzen und somit dem Gemeinwohl und dem Grundrechtsschutz zu dienen?
17. Welche Maßnahmen ergreift die Bundesregierung, um den Kryptografiestandort Deutschland für Nachwuchsfachkräfte attraktiv zu gestalten?
18. Hat die Bundesregierung eine Lösung für das Problem, dass zur Abwehr von konkreten, durch die Entwicklung von Quantentechnologien möglichen Gefahren auf die heutige und zukünftige IT-Kommunikation die Erlangung technologischer Souveränität in diesem Bereich notwendig ist, und inwieweit spielen entsprechende Überlegungen bei der Förderung von Quantentechnologien, insbesondere bezüglich Quantencomputer und Quantenkryptographie, eine Rolle?
19. Hält die Bundesregierung an der Notwendigkeit des staatlichen Handels mit Sicherheitslücken fest, die, wenn sie nicht geschlossen werden, auch (kriminellen) Dritten offenstehen, und sieht die Bundesregierung, dass hierdurch neue Gefahren für die IT-Sicherheit potentiell Millionen Betroffener entstehen können?

20. Wäre nach Ansicht der Bundesregierung eine zielgerichtete Abwehr konkreter Gefahren nicht sehr viel gebotener, als auf den staatlichen Handel mit Sicherheitslücken und generelle Hintertüren in Messenger-Diensten zu setzen?

21. Hat sich die Bundesregierung mit dem Problem befasst, dass es rechtsstaatlich geboten wäre, die Eingriffsschwellen zu erhöhen und die Transparenz und die parlamentarische Kontrolle des Einsatzes sogenannter „Staatstrojaner“ im Polizeibereich zu verbessern – statt dieses verfassungsrechtlich hochumstrittene Instrument auf den Nachrichtendienstbereich auszuweiten, und wenn nein, warum nicht?

22. Warum wartet die Bundesregierung nicht, bevor sie den Einsatz sogenannter „Staatstrojaner“ Bundespolizei und Nachrichtendiensten ermöglicht, das anstehende Urteil des Bundesverfassungsgerichts hierzu ab?

23. Hat die Bundesregierung rechtlich geprüft, ob es sich bei der geplanten Ausweitung des Einsatzes sogenannter „Staatstrojaner“ allein um die Ermöglichung der sogenannten Quellen-TKÜ handelt, oder soll darüber hinaus auch mehr als nur laufende Kommunikation überwacht werden, und handelt es sich demnach doch um eine Art „Online-Durchsuchung“, wie derzeit unter anderem in § 19 Absatz 6 des Referentenentwurfs zur Änderung des BND-Gesetzes (BNDG-RefE) zu lesen ist?

24. Wann wird die Bundesregierung die Zusammenarbeit mit einschlägigen IT-Sicherheitsfirmen beenden, von denen heute pressebekannt ist, dass sie ihre – mit öffentlichen Geldern gecodeten – Programme nach Ansicht der Fragesteller offenbar auch unter Umgehung bestehender Kontroll- und Exportregulierungsregime in autoritäre Staaten verkauften, beenden, und gegen die der Verdacht auf illegale Exporte besteht (vgl. „Verdacht auf illegale Exporte – Razzia bei Spionage-Firma FinFisher tagesschau.de vom 14. Oktober 2020, abrufbar unter: https://www.tagesschau.de/investigativ/ndr/spaehsoftware-finfisher-101.html)?

25. Teilt die Bundesregierung die Ansicht der Fragestellenden, dass es auch aus sicherheitspolitischen Überlegungen dringend angeraten ist, Programme, die in einem extrem grundrechtssensiblen Feld zum Einsatz kommen, zumindest staatlicherseits selbst zu entwickeln und, wo dies noch immer nicht möglich ist, auf den Einsatz zu verzichten, und wenn nein, warum nicht?

26. Hält die Bundesregierung ihre bisherige Kryptopolitik nach dem Leitsatz „Mehr Sicherheit durch und trotz Verschlüsselung“ für zeitgemäß, oder teilt sie die Ansicht der Fragestellenden, dass man als Demokratien im digitalen Zeitalter um eine Grundsatzentscheidung bezüglich der Frage, wie man zur grundgesetzlich garantierten Vertraulichkeit von Kommunikation und zur Kryptografie steht, nicht umhinkommt?

    Falls zweiteres, welche Bemühungen hat die Bundesregierung auf europäischer und internationaler Ebene unternommen, um sich mit anderen Staaten mit dem Ziel zusammenzuschließen, die Vertraulichkeit von Kommunikation durch Kryptografie zu stärken?

27. Inwiefern kann die Bundesregierung Berichte bestätigen, dass die EU – auf Vorschlag der Deutschen Ratspräsidentschaft – künftig eng mit der Geheimdienstallianz der Five Eyes sowie Indien und Japan zusammenarbeiten soll, um sichere Verschlüsselung in digitaler Kommunikation zu umgehen (vgl. https://www.sueddeutsche.de/digital/geheimdienste-verschluesselung-crypto-wars-messenger-1.5131084)?

28. Wie unterscheiden sich die Aufgabenfelder von ZITiS und der „Agentur für Innovation in der Cybersicherheit“ konkret?

29. Bleibt die Bundesregierung auch angesichts aktueller Berichterstattungen, nach denen ZITiS verschiedenen deutschen Sicherheitsbehörden, darunter Bundeskriminalamt (BKA), Bundespolizei, Bundesamt für Verfassungsschutz (BfV) und Bundesnachrichtendienst (BND) – auch in laufenden Strafverfahren – dabei hilft, die Verschlüsselung von Computern und Smartphones zu umgehen und den Zugriff auf gespeicherte Daten zu ermöglichen (vgl. „Mysterium ZITiS – Was macht eigentlich die „Hackerbehörde“?, tagesschau.de vom 26. Oktober 2020, abrufbar unter https://www.tagesschau.de/Investigativ/wdr/zitis-107.html), auch weiterhin bei der Ansicht, dass ZITiS allein „Dienstleister für die Sicherheitsbehörden des Bundes“ (vgl. Eigenbeschreibung ZITiS, abrufbar unter https://www.zitis.bund.de/DE/Home/home_node.html) ist und derartige Praktiken vom Errichtungserlass rechtlich gedeckt sind, und wenn ja, mit welcher aktuellen Begründung (vgl. Antwort der Bundesregierung auf die Mündlichen Fragen 78 und 79 des Abgeordneten Konstantin von Notz in der Fragestunde im Bundestag am 4. November 2020)?

30. Wie konkret kann die Bundesregierung vor dem Hintergrund ihrer Ausführungen, ZITiS stelle lediglich die Rechenkapazität des Hochleistungsrechners und das notwendige Fachwissen zur Bedienung zur Verfügung (vgl. ebd.) ausschließen, dass Mitarbeiterinnen und Mitarbeiter doch Kenntnis von Daten aus laufenden Verfahren haben (vgl. ebd.)?

31. Welche Sicherungsmechanismen gibt es hier, und wie wird rechtssicher ausgeschlossen, dass Mitarbeiterinnen und Mitarbeiter von ZITiS nicht doch Kenntnis von Daten aus laufenden Verfahren oder Passwörter von Beschuldigten erhalten?

32. Wie viele derartige „Ausnahmefälle“ gab es, in denen ZITiS im Rahmen eines Strafverfahrens für eine konkrete Dienstleistung angefragt wurde und ZITiS als „behördlicher Verwaltungshelfer“ zuarbeitete (vgl. ebd., bitte alle Fälle samt Datum und Behörde nennen)?

33. Hat die Bundesregierung geprüft, ob die Rechtmäßigkeit auch dann noch gegeben ist, wenn Mitarbeiterinnen und Mitarbeiter von ZITiS Kenntnis von Daten aus laufenden Verfahren hätten?

    Wenn ja, mit welchem Ergebnis?

    Und wenn nein, warum nicht?

34. Wäre die Rechtmäßigkeit nach Ansicht der Bundesregierung auch dann noch gegeben, wenn ZITiS auch Landespolizeien und Verfassungsschutzämtern entsprechende Unterstützung böte, und gab es in der Vergangenheit nach Kenntnis der Bundesregierung entsprechende Anfragen und/oder Kooperationen?

    Wenn ja, welche konkret (bitte nach Datum, Behörde und Art aufschlüsseln) (vgl. „Mysterium ZITiS – Was macht eigentlich die „Hackerbehörde“?, tagesschau.de vom 28. Oktober 2020, abrufbar unter https://www.tagesschau.de/investigativ/wdr/zitis-107.html)?

35. Wann ist nach Einschätzung der Bundesregierung bei ZITiS die Grenze zwischen Hilfeleistung in Einzelfällen und Ausnahmesituationen und einer regelmäßigen Unterstützungen auch von Landespolizeien und Verfassungsschutzämtern überschritten?

36. Kann die Bundesregierung bestätigen, dass ZITiS „erst eine Lücke entdeckt“ hat und diese dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet wurde, wenn ja, was geschah des Weiteren mit die-

ser Sicherheitslücke, nach welchem Zeitraum wurde sie geschlossen, falls nicht, welche gegenteiligen Erkenntnisse liegen der Bundesregierung über von ZITiS gefundene, erworbene, an Sicherheitsbehörden und/oder das BSI weitergegebene Sicherheitslücken vor (vgl. „Der Staat und seine Hacker“, SZ vom 16. November 2020)?

37. Mit welchen Firmen kooperieren ZITiS und die Bundeswehr, wenn es darum geht, Sicherheitslücken in IT-Produkten zu kaufen und/oder für den Einsatz durch Sicherheitsbehörden nutzbar zu machen (bitte konkret benennen)?

38. Plant die Bundesregierung, für alle Behörden und öffentlichen Stellen eine staatliche Meldepflicht für (bestimmte beispielsweise bislang nicht entdeckte) Sicherheitslücken einzuführen?

    Falls ja, wann soll eine solche Regelung kommen, und wie soll diese konkret ausgestaltet werden?

    Falls nicht, warum nicht?

39. Plant die Bundesregierung, weiterhin nach Vorbild des „Vulnerabilities Equities Process“ in den USA, einen Prozess zu etablieren, nachdem Sicherheitslücken bewertet werden, um diese – je nach Bewertung – entweder für Sicherheitsbehörden nutzbar zu machen oder diese umgehend an die Hersteller zu melden?

    Falls ja, in welchem Stadium befindet sich dieser Prozess, und wann ist mit der Vorlage zu rechnen?

40. a) Was ist der konkrete Stand bezüglich eines seit Langem in Erarbeitung befindlichen Erlasses für ein sogenanntes Schwachstellen-Management, an dem das Bundesministerium des Innern, für Bau und Heimat (BMI), und wann ist mit der Vorlage zu rechnen?

    b) Was genau wird der genaue Regelungsgegenstand des Erlasses sein, und auf welche Sicherheitslücken wird er sich konkret beziehen?

    c) Ist zutreffend, dass der Erlass allein für die dem BMI nachgeordneten Behörden gelten soll, und ist demnach auch nicht vorgesehen, dass andere Ministerien oder der Bundestag an der Erarbeitung eines solchen „Schwachstellen-Managements“ beteiligt werden sollen?

    d) Hält die Bundesregierung diese Vorgehensweise und einen Erlass, der allein auf die nachgeordneten Behörden eines Ministeriums zielt, für der Bedeutung des Themas angemessen, und wird sich die Bundesregierung zumindest für entsprechende Erlasse aller Ministerien einsetzen?

41. Welche Kenntnisse liegen der Bundesregierung vor dem Hintergrund, dass ZITiS in der Vergangenheit unter anderem dem Bundeskriminalamt (BKA) im Rahmen des „Projekt SMART“ Unterstützung „bei der Entwicklung einer Quellen-TKÜ-Lösung für mobile Endgeräte“, also bei der Entwicklung eines sogenannten „Staatstrojaners“ (RCIS) geleistet hat (vgl. „36 Mio. Euro – ZITiS baut Supercomputer zur Entschlüsselung“ auf netzpolitik,org vom 16. Oktober 2018, abrufbar unter https://netzpolitik.org/2018/36-millionen-euro-zitis-baut-supercomputer-zur-entschluesselung/), bezüglich weiterer Fälle vor, bei denen ZITiS an der Entwicklung sogenannter „Staatstrojaner“ beteiligt war oder ist, wie dies eine entsprechende Äußerungen des Präsidenten nahelegt, wenn ja, welche Behörden hat man hier wann im Rahmen welcher Projekte wie konkret unterstützt (vgl. „Der Staat und seine Hacker“ SZ vom 16. November 2020) (bitte konkret aufschlüsseln)?

42. In wie vielen Fällen wurden die dem Bundeskriminalamt zur Verfügung stehenden sogenannten „Staatstrojaner“, von denen drei inzwischen für den Einsatz freigegeben worden sind,

    a) in Strafverfahren und

    b) zur Gefahrenabwehr eingesetzt,

    und wie stellt sich das Verhältnis des Einsatzes von BKA-Eigenentwicklungen und eingekauften Produkten dar?

43. Welche Rolle wird ZITiS bei dem von der Bundesregierung geplanten Einsatz sogenannter Staatstrojaner durch Bundespolizei und Nachrichtendiensten spielen?

    Sind hier Hilfestellungen (wenn ja, wie konkret) oder Eigenentwicklungen geplant, oder wird ZITiS ggf. beraten, welche Produkte auf dem kommerziellen Markt erhältlich sind?

44. An welchen Projekten auf EU-Ebene, die das Ziel verfolgen, Kryptografie zu brechen, war und/oder ist ZITiS wie konkret beteiligt (vgl. „Mysterium ZITIS – Was macht eigentlich die „Hackerbehörde“?, tagesschau.de vom 28. Oktober 2020, abrufbar unter https://www.tagesschau.de/investigativ/wdr/zitis-107.html)?

45. An welchen Projekten hat ZITiS gearbeitet oder arbeitet ZITiS derzeit, die das Ziel verfolgen, Hintertüren in sogenannten Geräten des „Internet of Things“ zu finden und diese für Sicherheitsbehörden nutzbar zu machen (vgl. ebd., bitte Projekte konkret aufschlüsseln)?

46. An welchen Projekten hat ZITiS gearbeitet oder arbeitet ZITiS derzeit konkret, die das Ziel verfolgen, Sicherheitsbehörden Zugang zu Kommunikationen über Ende-zu-Ende-verschlüsselte Messenger-Dienste wie Telegram zu verschaffen (bitte Projekte konkret aufschlüsseln)?

47. a) Wodurch ist nach Auffassung der Bundesregierung eine nach Ansicht der Fragesteller derart hohe Honorarsumme für ein einziges Gutachten zum Thema („Unterstützung bei der Technologievorausschau und -bewertung – ‚Trendstudie‘“) an einen einzelnen Gutachter sachlich gerechtfertigt?

    b) Wann genau im Jahr 2020 hat ZITiS dieses Gutachten beauftragt?

    c) Bis wann soll dieses Gutachten vertragsgemäß abgeliefert werden?

48. a) Bei welchen Vertragspartnern wurden die anderen Gutachten in Auftrag gegeben (2018: „Rechtsgutachten zur Aufgabenerfüllung der ZITiS“; 2019: „Erweiterung des erstellten Rechtsgutachtens zur Aufgabenerfüllung der ZITiS um die Fragestellung zur Aufnahme von ZITiS in die Sicherheitsüberprüfungsfeststellungsverordnung“; 2020: „Rechtsgutachten Suchdienst Darknet“; zwei (?) Gutachten „Unterstützung bei der Technologievorausschau und -bewertung – ‚Trendstudie‘“, von denen eins von Roland Berger GmbH erstellt wurde)?

    b) Was waren die konkreten Ergebnisse der jeweiligen Gutachten?

    c) Wird die Bundesregierung dem Parlament die Gutachten – ggf. in eingestufter Form – zur Kenntnis geben?

Berlin, den 15. Dezember 2017

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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