Bundesministerium
des Innern, für Bau
und Heimat

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

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117
FAX +49 (0)30 18 681-11019

INTERNET www.bmi.bund.de

DATUM 1. Februar 2021

BETREFF **Kleine Anfrage des Abgeordneten Dr. Konstantin von Notz u. a. und der Fraktion Bündnis 90/Die Grünen**

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

BT-Drucksache 19/25549

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

Hinweis:

Ein Teil der Antwort ist VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft.

Mit freundlichen Grüßen
in Vertretung

Dr. Markus Richter

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin
VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof
Bushaltestelle Berlin Hauptbahnhof

Kleine Anfrage des Abgeordneten Dr. Konstantin von Notz u. a.
und der Fraktion Bündnis 90/Die Grünen

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

BT-Drucksache 19/25549

Vorbemerkung der Fragesteller:

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 im Stande 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. Kleine Anfrage 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 hoch widersprüchlich. 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:

Vorbemerkung der Bundesregierung:
Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt, soweit parlamentarische Anfragen jedoch Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen eine Beantwortung sämtlicher Fragen in offener Form nur teilweise erfolgen kann.

Im Einzelnen:

Die Antworten zu den Fragen 32, 34 und 42 sind in Teilen als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft. Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Behörden des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Fragen betreffen zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus dem Bekanntwerden der Antworten könnten Rückschlüsse auf Vorgehensweise, Fähigkeiten und Methoden

der Sicherheitsbehörden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.
Deshalb sind die Antworten zu den genannten Fragen gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (VS-Anweisung – VSA) in Teilen als „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Die Beantwortung der Fragen 37 und 41 berühren in besonders hohem Maße das Staatswohl. Nach sorgfältiger Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass auch das geringfügige Risiko ihrer Offenlegung nicht getragen werden kann und deshalb die Fragen hinsichtlich der Sicherheitsbehörden des Bundes mit polizeilichen und nachrichtendienstlichen Aufgaben auch nicht in eingestufter Form beantwortet werden können.

Eine Bekanntgabe von Einzelheiten der bei diesen Behörden zur Bekämpfung von Kriminalität und Terrorismus im Rahmen ihrer jeweiligen Zuständigkeit eingesetzten Softwareprodukte für die Bearbeitung und Auswertung von Ermittlungsverfahren würde weitgehende Rückschlüsse auf die technischen Fähigkeiten sowie die taktischen Einzelheiten bzw. Arbeitsabläufe und damit mittelbar auch sowohl auf die derzeitige als auch die geplante technische Ausstattung sowie das Strafverfolgungs- und Gefahrenabwehrpotenzial dieser Behörden zulassen.
Das Benennen eines Unternehmens gegenüber einer nicht überschaubaren Öffentlichkeit im Kontext polizeilicher und nachrichtendienstlicher Arbeit kann das betroffene Unternehmen in seinem Bestand gefährden. Zum einen könnten Dritte von Geschäftsbeziehungen mit diesem Unternehmen Abstand nehmen. Zum anderen könnte eine Benennung Rückschlüsse auf den Entwicklungsstand und Arbeitsweisen des Unternehmens zulassen, wodurch dessen Wettbewerbsfähigkeit beeinträchtigt sein könnte.
Weiterhin könnte das Bekanntwerden einer (Geschäfts-)Beziehung eines Unternehmens zu den Bundesbehörden das Unternehmen zum Ziel von Aufklärungsbemühungen fremder Mächte machen. Hierdurch entstehende Wissensabflüsse wären einerseits schädlich für das Unternehmen. Sie beeinträchtigen andererseits aber auch die Funktionsweise und Arbeitsfähigkeit der Bundesbehörden, da eine Zusammenarbeit mit Unternehmen für deren Arbeit oftmals unerlässlich ist.
Ferner berühren diese Fragen unmittelbar Aspekte zu technischen Vorgehensweisen und Fähigkeiten der polizeilichen und nachrichtendienstlichen Behörden auf dem Gebiet der informationstechnischen Überwachung. Durch ein Bekanntwerden dieser

Methoden könnten die Fähigkeiten der Sicherheitsbehörden mit polizeilichen und nachrichtendienstlichen Aufgaben, Erkenntnisse im Wege der technischen Strafaufklärung und Gefahrenabwehr zu gewinnen, in erheblicher Weise negativ beeinflusst werden, insbesondere, wenn keine ausreichenden Alternativen zu den für die Strafverfolgung und Gefahrenabwehr genutzten Produkten zur Verfügung stehen. Denn Beschuldigte könnten sich somit gezielt eben jener Strafverfolgung und Gefahrenabwehr entziehen, etwa durch Maßnahmen zur Hinderung des Einsatzes der entsprechenden Software. Dies ist jedoch nicht hinnehmbar, da die IT- bzw. softwaregestützte Gewinnung von Informationen für die Aufgabenerfüllung der Strafverfolgung und Gefahrenabwehr dieser Behörden und damit für die Sicherheit der Bundesrepublik Deutschland und bei der Bekämpfung vor allem des Terrorismus, der politisch motivierten sowie der organisierten Kriminalität unerlässlich ist. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies würde folgenschwere Einschränkungen der Strafverfolgung und Gefahrenabwehr bedeuten, womit letztlich die gesetzlichen Aufträge von Bundeskriminalamt (BKA) – verankert im Grundgesetz (GG) (Art. 73 Abs. 1 Nr. 10 GG, Art. 87 GG) und im Bundeskriminalamtgesetz (BKAG), Bundespolizei (BPOL) (Art. 87 GG sowie Bundespolizeigesetz [BPolG]) und Zollkriminalamt (ZKA)/Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit [FIU]) (Art. 87 GG, Zollfahndungsdienstgesetz (ZFdG), Geldwäschegesetz (GwG), Unionszollkodex (UZK) – nicht mehr sachgerecht erfüllt werden könnten.

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

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Informationen sowohl für die Aufgabenerfüllung der Nachrich-

tendienste des Bundes als auch der Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, mittels welcher technischen Produkte die Sicherheitsbehörden z. B. von der Telekommunikationsüberwachung Gebrauch machen, könnte zu einer Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, die eine weitere Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

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?

Zu 1:
Traditionelle Hochleistungsrechner stellen bei geeigneten Schlüssellängen keine direkte Bedrohung für die heute vom Bundesamt für Informationstechnik im Sicherheitsbereich (BSI) in der Technischen Richtlinie TR-02102 empfohlenen kryptografischen Algorithmen dar. Denkbar ist es, sie für Seitenkanalangriffe auf Implementierungen kryptografischer Mechanismen einzusetzen. Dabei könnten auch KI-Methoden zum Einsatz kommen. Grundsätzlich sind nach heutigem Forschungsstand die in der TR-02102 des BSI empfohlenen symmetrischen Verschlüsselungsverfahren, z. B. Advanced Encryption Standard (AES-256), nicht durch Quantencomputer gefährdet. Quantencomputer würden die heute verwendete Public-Key-Kryptografie gefährden. Asymmetrische Verfahren zur Schlüsseleinigung und zur Digitalen Signatur beruhen auf dem Faktorisierungsproblem oder dem Diskreten Logarithmus-Problem und lassen sich deswegen potentiell mit dem Algorithmus von Shor angreifen. Zur Einschätzung dieser Gefahr hat das BSI eine Studie durchgeführt

(www.bsi.bund.de/qcstudie), deren Fortführung geplant ist. Im Hochsicherheitsbereich arbeitet das BSI unter der Hypothese, dass Anfang der 2030er Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen werden. Diese Aussage ist nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen, sondern stellt einen Richtwert für die Risikobewertung dar. Solange die Daten in Datenbanken symmetrisch verschlüsselt sind und der Zugriff geeignet abgesichert ist, erscheinen Angriffe mit Quantencomputern heute unrealistisch.
Es bleibt die Frage der Langzeitsicherheit von kryptografischen Algorithmen. Grundsätzlich kann für keinen der heute verwendeten kryptografischen Algorithmen ausgeschlossen werden, dass er zukünftig mit neuen Methoden gebrochen wird. Dies gilt insbesondere auch für die in Blockchains verwendeten kryptografischen Algorithmen. Die mit diesen verbundenen kryptografischen Herausforderungen werden in der Publikation "Blockchain sicher gestalten. Konzepte. Anforderungen. Bewertungen." des BSI analysiert.

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?

Zu 2:
In der Quantenkommunikation sieht die Bundesregierung eine Schlüsseltechnologie zur Sicherung der technologischen Souveränität Deutschlands. Sichere Kommunikationsnetzwerke haben in modernen Informationsgesellschaften den Stellenwert einer kritischen Infrastruktur. Quantenkommunikation kann unsere Gesellschaft auch zukünftig vor Gefährdungen durch Cyberangriffe und Datenlecks schützen. Kryptoagilität ist aus Sicht der Bundesregierung ein sehr wichtiger Aspekt, nicht nur im Hinblick auf Quantencomputer. Wesentliche Bausteine, um Kryptoagilität zu erreichen, sind hashbasierte Signaturverfahren, da sie die Möglichkeit bieten, Soft- und Firmwareupdates quantencomputerresistent zu signieren. Das BSI empfiehlt bereits jetzt hashbasierte Signaturverfahren zur Absicherung von Soft- und Firmwareupdates und wird diese auch in die TR-02102 aufnehmen. Um Interoperabilität zu erleichtern, wird dazu die Special Publication 800-208 des National Institute of Standards and Technology (NIST), Recommendation for Stateful Hash-Based Signature Schemes vom Oktober 2020 herangezogen. Für Satelliten sind hashbasierte Signaturen bereits in der TR-03140 des BSI zum Satellitendatensicherheitsgesetz (SatDSigG) vorgesehen. Zukünftig ist ebenfalls geplant, sogenannte Stateless Hash-Based Signatures

(SPHINCS+) zu empfehlen, sobald ein anerkannter Standard existiert. Ein weiterer Aspekt, der ein flexibleres Design ermöglicht, ist der Einsatz von hybriden Verfahren beispielsweise für eine Schlüsseleinigung. Hybrid meint hier, dass ein quantencomputerresistentes Verfahren mit einem "klassischen" Verfahren kombiniert wird. Dies ist zumindest für eine Übergangsphase bei der Migration zu Post-Quanten-Kryptografie eine Möglichkeit, um sich bereits frühzeitig gegen die Bedrohung durch Quantencomputer abzusichern und gleichzeitig noch den Schutz durch gut untersuchte und standardisierte Verfahren zu nutzen. Zudem bietet die Etablierung von hybriden Lösungen zukünftig die Möglichkeit eines flexibleren Austausches von abgekündigten bzw. unsicheren Verfahren.
Darüber hinaus ist die Kryptoagilität ein wichtiger Forschungsgegenstand des Förderschwerpunkts zur Post-Quanten-Kryptographie der Bundesregierung.

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)?

Zu 3:
Technologische Souveränität ist ein Kernthema der Forschungsförderung der Bundesregierung und spielt daher eine wichtige Rolle bei den Fördermaßnahmen. Im Bereich der Kryptographie fördert das Bundesministerium für Bildung und Forschung (BMBF) die in der Antwort zu Frage 6 genannten Projekte.
Das BMBF und das französische Forschungsministerium (MESRI) haben sich auf dem 6. Forum zur deutsch-französischen Zusammenarbeit in Berlin verständigt, eine starke deutsch-französische Forschungsachse zur Cybersicherheit zu entwickeln. Die „Richtlinie zur Förderung von deutsch-französischen Verbundprojekten zur Cybersicherheit“ vom 7. November 2019 setzt die Empfehlungen des Forums um. Ziel der Förderung ist es, hochinnovative Lösungen zur Wahrung der Privatsphäre zu entwickeln, die insbesondere in den drei Anwendungsbereichen Industrie 4.0 (einschließlich Internet of Things), Gesundheitswesen und Automotive besonderen Nutzen erreichen. Acht deutsch-französische Verbundprojekte wurden zur Förderung ausgewählt; die Projekte starten voraussichtlich im 2. Quartal 2021. Folgende Projekte haben u. a. einen Forschungsschwerpunkt im Bereich Kryptografie:

- APRIORI: Advanced Privacy of IOT Devices through Robust Hardware Implementations
- AUTOPSY: Automotive data-tainting for Privacy Assurance System
- CRYPTECS: Cloud-Ready Privacy-Preserving Technologies
- Pivot: Privacy-Integrated design and Validation in the constrained IoT
- PROPOLIS: Privacy for smart cities
- TinyPART: Tiny, private, proved and isolated
- UPCARE: User-Centric and Privacy-Preserving Cancer Research Platform

Flankierend entwickelt das BSI in Zusammenarbeit mit ETSI Prüfkriterien für Geräte zur Quantum-Key-Distribution. Ziel ist dabei, Prüfkriterien für das CC-Level EAL 4+ zu entwickeln. Detailliert werden diese Aktivitäten bereits in der Antwort der Bundesregierung auf eine frühere Kleine Anfrage zur Förderung von Quantentechnologien Bundestagsdrucksache 19/25208 beschrieben.
Darüber hinaus wird auf die Antwort zu Frage 18 verwiesen.

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?

Zu 4:
Das BMBF fördert derzeit sieben Forschungsprojekte zur Post-Quanten-Kryptographie (siehe Antwort zu Frage 6) mit ca. 16 Millionen Euro, die Ende 2019 gestartet sind. Eine Fortsetzung dieses Förderschwerpunkts ist geplant.

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?

Zu 5:
Die Bundesregierung geht grundsätzlich davon aus, dass sich Post-Quanten-Kryptografie innerhalb der nächsten Jahre in allen Produkten, die kryptografische Mechanismen nutzen, durchsetzen wird. Dazu wird es aber in der Breite erst kommen, wenn etablierte Standards zur Verfügung stehen. Der Aufwand für die Migration auf die neuen Verfahren und entsprechende Anpassung kryptografischer Protokolle, z. B. Transport Layer Security (TLS), Internet Protocol Security (IPsec), X.509 für digitale Signaturen, ist allerdings keinesfalls zu unterschätzen. Als Maßnahme gegen die Bedrohung der Public-Key-Kryptografie durch Quantencomputer arbeitet das BSI für den Hochsicherheitsbereich zurzeit an der Migration zu Post-Quanten-Kryptografie. Im April 2020 hat das BSI dazu erste Handlungsempfehlungen auf seiner Webseite veröffentlicht (siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html), deren Erweiterung für 2021 geplant ist.

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)?

Zu 6:
Die Bundesregierung geht davon aus, dass die Frage sich auf asymmetrische RSA Verschlüsselung bezieht. Hierzu wird bezüglich der Verwendung von Quantencomputern zunächst auf die Antwort der Bundesregierung auf Frage 5d) der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Förderung von Quantentechnologien auf Bundestagsdruckasche 19/25208 verwiesen. Ein Brechen von RSA allein mit Hochleistungsrechnern und ohne Ausnutzung von Seitenkanälen wird bei geeigneten Schlüssellängen als im Moment nicht realistisch angesehen. Das BSI betreibt hierzu selbst keine Forschung, sondern verfolgt die wissenschaftliche Entwicklung. Darüber hinaus fördert das BMBF Forschungsvorhaben mit dem Ziel, Post-Quanten-Kryptographie und Quantenkommunikation zur Anwendungsreife zu bringen. Derzeit fördert das BMBF die folgenden Projekte:

- Post-Quanten-Kryptographie:
    - Aquorypt: Anwendbarkeit quantencomputerresistenter kryptografischer Verfahren

  - FLOQI: Full-Lifecycle-Post-Quantum-PKI
  - KBLS: Kryptobibliothek Botan für langlebige Sicherheit
  - PQC4MED: PQC Technologien für den Datenschutz in der medizinischen Versorgung in Deutschland
  - QuantumRISC: Kryptografie der nächsten Generation für eingebettete Systeme
  - QuaSiModO: Quanten-Sichere VPN-Module und -Operationsmodi
  - SIKRIN-KRYPTOV: Sicherung von hydraulischen Anlagen in kritischen Infrastrukturen durch Entwicklung und Implementierung Quantencomputer-resistenter kryptographischer Verfahren
- Quantenkommunikation:
  - Q.Link.X: Quantum Link Extended
  - QuNET: Quantentechnologien für sichere Netzwerke und Kommunikation
  - QUBE: Quantenschlüsselverteilung mit Cube-Sat
  - HYPER-U-P-S: Hyper-entanglement from ultra-bright photon pair sources
  - MICROSENS: MICROwave quantum SENSing with diamond color centers
  - QuICHE: Quantum information and communication with high-dimensional encoding
  - ShoQC: Short-range optical Quantum Connections

Auch das Forschungsinstitut CODE der Universität der Bundeswehr München (UniBw M) führt ein PostQuantenKryptographie (PQC) - Projekt mit der Firma Infineon durch. Der Titel lautet: „Erforschung effizienter Implementierung von Gitter-basierten kryptographischen Methoden für Sicherheitscontroller und eingebettete Microcontroller“.

7:

Welche Projekte verfolgt die Bundesregierung konkret, damit sensible Kommunikation zukünftig so verschlüsselt wird, dass sie nicht mit Quantencomputern nachträglich entschlüsselt werden kann?

Zu 7:

Es wird auf die Antwort zu Frage 6 verwiesen. Zudem umfassen die Aktivitäten des BSI unter anderem folgende Projekte:

- Einbau quantencomputerresistenter Verfahren zur Schlüsseleinigung in Produkte für den Hochsicherheitsbereich,
- Fortführung Studie zum "Entwicklungsstand Quantencomputer" als Grundlage für eine Risikoabschätzung,
- Studie zur "Bewertung gitterbasierter kryptografischer Verfahren".

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?

Zu 8:

Grundsätzlich vertritt die Bundesregierung die Position, dass im Allgemeinen Post-Quanten-Kryptografie zur Absicherung ausreichend ist, sodass Quantennetzwerke aus Sicherheitsperspektive in der Breite derzeit nicht erforderlich sind (vgl. die Antwort der Bundesregierung auf eine frühere Kleine Anfrage zur Förderung von Quantentechnologien Bundestagsdrucksache 19/25208).
Die Aktivitäten der Bundesregierung zum Aufbau eines Quantenkommunikationsnetzes werden in der Antwort auf eine frühere Kleine Anfrage zur Förderung von Quantentechnologien (Bundestagsdrucksache 19/25208) dargelegt. Voraussetzung für ein umfassendes Quantennetzwerk sind die Verfügbarkeit von Quantenrepeatern und von sicheren Geräten zum Quantenschlüsselaustausch (QKD) mit hinreichender Leistung aus deutscher oder europäischer Herkunft. Quantenrepeater werden gegenwärtig im Projekt Q.Link.X erforscht und sind noch nicht verfügbar. Prüfkriterien für QKD-Geräte werden vom BSI in Zusammenarbeit mit ETSI entwickelt, werden aber für Prepare-And-Measure-QKD sicher nicht vor 2023 zur Verfügung stehen. Prüfkriterien für Geräte, die verschränkungsbasierte QKD bieten, werden entsprechend später vorliegen. Im Sinne der digitalen Souveränität werden dann Produkte von (vertrauenswürdigen) Herstellern aus Deutschland oder der EU benötigt. Unabhängig davon sind Punkt-zu-Punkt-Verbindungen, bei denen QKD neben Post-Quanten-Kryptografie hybrid verwendet wird, schon heute denkbar.
Im Rahmen der Forschungsinitiative QuNET (Laufzeit voraussichtlich 2019 bis 2026) sollen die technologischen Grundlagen für künftige Quantenkommunikationsnetze in Deutschland geschaffen werden. Mit dieser Fördermaßnahme schafft das BMBF Zugang zu dieser Technologie für die deutsche IKT-Industrie.

Über das neu gegründete Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (DTEC.Bw) hat das Bundesministerium der Verteidigung (BMVg) zur Erforschung und zum experimentellen Nachweis nutzbarer Quantum Key Distribution Forschungsmittel für das Projekt MuQuaNet (Das Quanten-Kommunikationsnetz im Großraum München) mit einer Laufzeit von vier Jahren zur Verfügung gestellt. Im Rahmen dieses Projektes wird im Großraum München eine Quantenkommunikationsinfrastruktur aufgebaut. Ausgewählte sicherheitskritische zivile und militärische Anwendungsfälle werden implementiert und auf ihre Vertraulichkeit, Integrität, Verfügbarkeit und Wirtschaftlichkeit gegen Angriffe von Quantencomputern getestet.

9:
Inwiefern und welche Entwicklungen von quantencomputerresistenten kryptografischen Systemen werden durch staatliche Behörden entwickelt oder gefördert?

Zu 9:
Das BSI führt bei Produkten für den Hochsicherheitsbereich in Zusammenarbeit mit der deutschen Kryptoindustrie eine Migration zu quantencomputerresistenter Kryptografie durch.

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)?

Zu 10:
Das BSI empfiehlt in TR-02102 bereits heute zwei besonders konservative Algorithmen zur Schlüsseleinigung, die nach heutigem Kenntnisstand nicht durch Quantencomputer gebrochen werden können, nämlich FrodoKEM und Classic McEliece. Das National Institute of Standards and Technology (NIST) entwickelt derzeit Standards für quantencomputerresistente kryptografische Verfahren; die Bundesregierung geht davon aus, dass diese nicht vor 2024 finalisiert werden. Im Anschluss wird das BSI auch für Deutschland weitere Empfehlungen aussprechen. Eine Ausnahme ist die NIST SP 800-208, in der die von der IETF standardisierten, hashbasierten Signaturverfahren LMS und XMSS von NIST gutgeheißen werden. Bereits 2016 hat das BSI eine Studie zur "Bewertung gitterbasierter kryptografischer Verfahren" durchgeführt.

Gitterbasierte Kryptografie ist eine Klasse von Verfahren, die als quantencomputerresistent gelten. Das Verfahren FrodoKEM, das in der TR-02102 empfohlen wird, ist ein gitterbasiertes Verfahren zur Schlüsseleinigung. Insgesamt scheinen gitterbasierte Verfahren die vielversprechendsten Kandidaten im NIST-Prozess zu sein. Allerdings muss dabei unterschieden werden zwischen Verfahren, die auf sogenannten "strukturierten" Gittern beruhen und im Allgemeinen sehr effizient sind, und Verfahren, wie FrodoKEM, die auf unstrukturierten Gittern beruhen und dadurch wahrscheinlich ein höheres Sicherheitsniveau bieten. Das BSI gewichtet den potentiellen Sicherheitsgewinn von FrodoKEM zurzeit höher als die Effizienz anderer gitterbasierter Verfahren.

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)?

Zu 11:
Seitens der deutschen Sicherheitsbehörden sind weder Beta-Versionen noch Simulationen von Quantencomputern im Test oder Einsatz.

12:
Welche Art Hochleistungsrechner ist derzeit bei ZITIS im Einsatz?

Zu 12:
Der sich im Einsatz befindende Hochleistungsrechner der ZITiS ist ein Cluster aus Parallelrechnern mit unterschiedlichen Prozessorarchitekturen.

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?

Zu 13 und 14:
Die Fragen 13 und 14 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet. Über den Zugang des "IBM Q Hub" an der UniBw M haben aktuell neben universitätseigenen Wissenschaftlerinnen und Wissenschaftlern auch kleinere Forschungsgruppen des DLR einen Zugang zu den IBM-Quantencomputern. Im Rahmen von Studium und Lehre sowie von Hackathons haben auch Nutzerinnen und Nutzer der Ludwig-Maximilians-Universität München (LMU) und der Technischen Universität München (TUM) einen Zugang. Schließlich haben oder hatten Gruppen der Hochschule München, der Hochschule Münster und der Fachhochschule Oberösterreich (Hagenberg/Österreich) einen Zugang zu „IBM Q Systemen“. Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften prüft überdies, ob ein dauerhafter Zugang zum „IBM Q Hub“ und den „IBM Q Systemen“ abgebildet werden kann. ZITiS ist nicht in dieses Projekt involviert. Allerdings besteht zwischen der ZITiS und dem Forschungsinstitut Cyber Defense („FI CODE“) der UniBw M ein akademischer Austausch zum Thema Quantentechnologien.

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?

Zu 15 und 16:
Die Fragen 15 und 16 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung hat sich (bereits im Jahr 1999, Kabinettbeschluss „Eckpunkte der deutschen Kryptopolitik“) gegen jegliche Schwächung, Modifikation oder ein Verbot von Verschlüsselung oder ein Kompromittieren von Sicherheitsstandards der digitalen Kommunikation bekannt. Dies hat weiterhin Bestand. Aus diesem Grund fördert die Bundesregierung Forschungsvorhaben, um quantencomputerresistente Kryptografie und Quantenkommunikation zur Anwendungsreife zu bringen und langfristig den Schutz von Daten im Sinne von Gemeinwohl und Grundrechtsschutz zu gewährleisten.
Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden aber nicht ausgehöhlt werden. Diese Behörden müssen unter strengen gesetzlichen Voraussetzungen befugt und in der Lage sein, verschlüsselte Kommunikation in Einzelfällen zu entschlüsseln oder zu umgehen, wenn dies zur Aufklärung schwerster Straftaten oder zum Schutz der Bevölkerung vor großen Gefahren notwendig ist. Vor diesem Hintergrund hat der Gesetzgeber in engem Umfang gesetzliche Befugnisse etwa für Maßnahmen der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung geschaffen. Das steht auch nicht im Widerspruch zum Ziel der Bundesregierung (Digitale Agenda von 2014), Deutschland zum „Verschlüsselungsstandort Nr. 1“ weiter auszubauen.

17:
Welche Maßnahmen ergreift die Bundesregierung, um den Kryptografiestandort Deutschland für Nachwuchsfachkräfte attraktiv zu gestalten?

Zu 17:
Forschung in den durch die Bundesregierung geförderten Projekten stellt ein attraktives Betätigungsfeld für Nachwuchsfachkräfte dar, z. B. in Form von Doktorarbeiten oder Stellen für Nachwuchsgruppenleiterinnen und -leiter. Auch in den vom BMBF institutionell geförderten Kompetenzzentren für IT-Sicherheitsforschung ATHENE, CISPA und KASTEL findet intensive Forschung zu Kryptographie statt, wobei Nachwuchsfachkräfte ihre akademische und persönliche Weiterentwicklung in einem exzellenten wissenschaftlichen Umfeld vertiefen können.

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?

Zu 18:

Im Bereich der Quantenkommunikation ist technologische Souveränität eine Grundlage für den Aufbau vertrauenswürdiger Kommunikationsnetze.
Technologische Souveränität in der Quantenkommunikation ist aus Sicht der Bundesregierung unerlässlich und daher u. a. Ziel der Forschungsförderung. Die Bundesregierung fördert nationale Forschungsvorhaben mit dem Ziel, Post-Quanten-Kryptografie und Quantenkryptografie zur Anwendungsreife zu bringen. Ziel ist es, den Schutz von Daten auch im Angesicht der fortschreitenden Entwicklung von Quantentechnologien zu wahren, in diesen Bereichen Deutschlands technologische Souveränität zu sichern und zu einem Innovationsmotor der Europäischen Union zu werden.

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?

Zu 19 und 20:

Die Fragen 19 und 20 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet. Die Bundesregierung plant nicht und setzt sich auch nicht für einen staatlichen Handel mit Sicherheitslücken ein. Als Cyber-Sicherheitsbehörde des Bundes wirkt vielmehr das BSI gemäß seinem aus § 3 Abs. 1 BSI-Gesetzes hervorgehenden gesetzlichen Auftrag darauf hin, sämtliche Sicherheitslücken umgehend und im ver-

trauensvollen Austausch mit den Technologieherstellern zu schließen. Darüber hinaus setzt sich die Bundesregierung derzeit inhaltlich mit der Thematik eines verantwortungsvollen Schwachstellenmanagements auseinander. Die Meinungsbildung innerhalb der Bundesregierung hierzu ist nicht abgeschlossen.

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?

Zu 21:

Die Bundesregierung geht bei der Beantwortung dieser Frage davon aus, dass diese auf den Einsatz von Programmen zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung durch Polizeibehörden gemäß den geltenden gesetzlichen Bestimmungen abzielt. Der Begriff „Trojaner" ist für solche Instrumente der informationstechnischen Überwachung ungeeignet, wie die Bundesregierung bereits im Rahmen der Beantwortung mehrerer Kleiner Anfragen, beispielsweise in der Bundestagsdrucksache 18/11261 zu Frage 13, Bundestagsdrucksache 19/1434 zu Frage 18 oder Bundestagsdrucksache 19/12465 zu Fragen 11 bis 11e dargestellt hat. Die Bundesregierung hält die geltenden bundesrechtlichen Bestimmungen im BKAG zur Quellen-Telekommunikationsüberwachung und zur Online-Durchsuchung einschließlich der betreffenden Eingriffsschwellen und den Regelungen zur richterlichen Kontrolle für verfassungsgemäß.
Darüber hinaus unterliegen verdeckte polizeiliche Maßnahmen des BKA der Berichtspflicht gegenüber dem Bundestag gemäß § 88 BKAG so dass auch in diesem Bereich eine parlamentarische Kontrolle erfolgt.
Des Weiteren entspricht nach Auffassung der Bundesregierung auch die im Regierungsentwurf zur Anpassung des Verfassungsschutzrechts enthaltene Regelung zur Quellen-Telekommunikationsüberwachung den verfassungsrechtlichen Vorgaben.

22:

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

Zu 22:
Instrumente der Quellen-TKÜ sind aus Sicht der Bundesregierung grundsätzlich erforderlich, um die Handlungsfähigkeit bei der Abwehr erheblicher Gefahren für herausragende Rechtsgüter und bei der Strafverfolgung im jeweiligen Aufgabenbereich zu erhalten. Eine entsprechende Befugnis ist nun im Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts vorgesehen. Die Bundesregierung ist der Auffassung, dass dieser Gesetzentwurf den verfassungsrechtlichen Anforderungen genügt.
Mit Blick auf die Bundespolizei setzt sich die Bundesregierung derzeit inhaltlich mit der Thematik auseinander. Die Meinungsbildung innerhalb der Bundesregierung hierzu ist nicht abgeschlossen."

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 BNDG-RefE zu lesen ist?

Zu 23:
Im Regierungsentwurf zur Anpassung des Verfassungsschutzrechts (Bundesratsdruckscahe 674/20) ist eine Regelung zur Quellen-TKÜ, nicht aber für die Online-Durchsuchung vorgesehen. Die Regelung in § 19 Abs. 6 BNDG-E ist den Befugnisnormen der Inlandsbehörden für die sogenannte „Quellen-TKÜ" nicht vergleichbar und stellt keine Befugnis zur „Online-Durchsuchung" dar.

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 (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)?

Zu 24:
Es wird auf die Antwort der Bundesregierung zur Schriftlichen Frage des Abgeordneten Dr. Konstantin von Notz auf Bundestagsdrucksache 19/23454, Nr. 52 verwiesen.

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?

Zu 25:
Bei besonders schützenswerten, mit einem hohen Risiko behafteten oder für die Handlungsfähigkeit der Strafverfolgungs- und Sicherheitsbehörden essentiellen Technologien und Fähigkeiten sollte die Bundesrepublik Deutschland zur Stärkung der Digitalen Souveränität eine krisenfeste Versorgungssicherheit anstreben. Staatliche Eigenentwicklung ist ein unverzichtbarer Teil, um dies gewährleisten zu können, um die Abhängigkeiten von Herstellern und Dienstleistern aus dem Nicht-EU-Ausland zu verringern und um das Einhalten gesetzlicher Vorgaben und der korrespondierenden ethischen Werte sicherzustellen. Damit die Sicherheitsbehörden nicht von den Ergebnissen des technologischen Fortschrittes abgekoppelt werden, muss es darüber hinaus möglich sein, dass sie sich moderner Verfahren und Entwicklungen aus globalen Lieferketten bedienen. Um dies gesichert und selbstbestimmt tun zu können, ist die für eine Bewertung, Prüfung und Betrieb notwendige Kompetenz ebenfalls staatlicherseits auf- bzw. auszubauen und zu erhalten.

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?

Zu 26:
Die Bundesregierung hat ihre grundsätzliche Haltung zum Thema Verschlüsselung in den Eckpunkten der deutschen Kryptopolitik (Kabinettbeschluss vom 2. Juni 1999) festgelegt. Danach hält die Bundesregierung an den als „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ bekannten Säulen der deutschen Kryptopolitik fest. Sie entsprechen der Cybersicherheitsstrategie 2016 der Bundesregierung und den Vorhaben des Koalitionsvertrags, neben dem berechtigten Schutz von Firmengeheimnissen und persönlichen Daten über die Stärkung und Förderung der Ende zu Ende-Verschlüsselung zugleich sicher zu stellen, dass die Strafverfolgungs- und Sicherheitsbehörden ihre bestehenden Befugnisse auch in der digitalen Welt anwenden und durchsetzen können. Hierfür gibt es keine einfachen technischen Lösungen, der Schwerpunkt muss auf der Notwendigkeit liegen, ein Gleichgewicht zwischen dem Schutz von Firmengeheimnissen und persönlichen Daten und den Bedürfnissen der Strafverfolgungs- und Sicherheitsbehörden zu erreichen.
In Bezug auf die Quantenkommunikation zählt Deutschland zu den ersten der mittlerweile 25 EU-Mitgliedstaaten, die die Vereinbarung zur Implementierung einer europäischen Quantenkommunikationsinfrastruktur (EuroQCI) unterzeichnet haben. Derzeit werden, gemeinsam mit den europäischen Partnern, Anforderungen an die künftige EuroQCI ausgearbeitet, die einen terrestrischen und einen satellitengestützten Bereich haben soll.

27:
Inwiefern kann die Bundesregierung Berichte bestätigen, dass die EU – auf Vorschlag der Deutschen Ratspräsidentschaft – künftig eng mit der Geheimdienstallianz der Five Eyessowie 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)?

Zu 27:
Die Bundesregierung kann diesen Bericht nicht bestätigen.

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

Zu 28:
Gemäß § 2 Absatz 2 des ministeriellen Errichtungserlasses (EE) vom 6. April 2017 hat die ZITiS die Aufgabe, Behörden des Bundes mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. ZITiS arbeitet somit als Stelle im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat (BMI) mit Schwerpunkt für die und abgestimmt mit den Sicherheitsbehörden des BMI. Stellen anderer Ressorts können an den Arbeitsergebnissen der ZITiS teilhaben. Der Schwerpunkt der ZITiS liegt in der Unterstützung der Sicherheitsbehörden BKA, BPOL und Bundesamt für Verfassungsschutz (BfV) im Hinblick auf Kriminalitätsbekämpfung sowie Gefahren- und Spionageabwehr in den eingangs genannten Bereichen. Dagegen ist die Agentur explizit für ressortübergreifende Vorhaben aufgestellt, mindestens der beiden Gründungsressorts BMI und BMVg. Die geförderten Forschungsthemen der Agentur betreffen die Cybersicherheit als Ganzes. Sie finanziert und beauftragt Forschungsvorhaben mit hohem Innovationspotenzial auf dem Gebiet der Cybersicherheit und diesbezüglicher Schlüsseltechnologien für die Bedarfsdeckung des Staates im Bereich der Inneren und Äußeren Sicherheit.

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 78/79 des Abgeordneten Konstantin von Notz in der Fragestunde im Bundestag am 4. November 2020)?

Zu 29:
Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) unterstützt, gemäß Errichtungserlass, die Behörden des Bundes mit Sicherheitsaufgaben in technischer Hinsicht unter anderem bei der Verwendung der entwickelten Produkte. Sofern zum Beispiel im Rahmen eines Strafverfahrens im Ausnahmefall eine konkrete

Dienstleistung angefragt wird, agiert ZITiS als behördlicher Verwaltungshelfer. Die Rechtsgrundlage des Errichtungserlasses ist hierfür weiterhin ausreichend auch wenn im konkreten Fall verfahrensbezogene Inhalte verarbeitet werden müssen. Auf die Ausführungen zu Frage 33 wird verwiesen.

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?

Zu 30 und 31:
Die Fragen 30 und 31 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet. Durch ein entsprechendes Sicherheitskonzept wird sichergestellt, dass durch geeignete technische Maßnahmen unberechtigte Zugriffe auf Daten sowohl auf Hardware- als auch Softwareebene nicht erfolgen können. Diese Maßnahmen umfassen unter anderem die physische und logische Trennung von Daten und die Implementierung eines umfassenden Rollen- und Rechtekonzeptes.

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)?

Zu 32:
ZITiS hat in 15 Fällen den Hochleistungsrechner genutzt, um im Rahmen von Amtshilfen als behördlicher Verwaltungshelfer zuzuarbeiten. Zu den zugrundeliegenden Ermittlungsverfahren liegen ZITiS keine Erkenntnisse vor.
Darüber hinaus wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

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?*

Zu 33:

Die ZITiS hat nach § 2 Abs. 1 Satz 1 des EE zur Aufgabe, Behörden des Bundes mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. § 2 Abs. 1 Satz 1 EE bezieht sich hingegen nicht auf Landesbehörden. Dennoch können Landesbehörden ihre Bedarfe an die Zentralstellen des BfV und BKA kommunizieren, welche wiederum ZITiS beauftragen können. Darüber hinaus unterhält und etabliert ZITiS nach § 2 Abs. 4 EE im Benehmen mit BfV und BKA Verbindungen zu Landesbehörden. Der ministerielle Errichtungserlass der ZITiS weist keinerlei Ermittlungsbefugnisse oder Befugnisse zum Eingriff in Grundrechte auf - ZITiS ist keine Ermittlungsbehörde und ist nicht operativ tätig. Wird ZITiS von einer dazu berechtigten Stelle in einem konkreten Ermittlungsverfahren einbezogen, greift der Charakter von ZITiS als behördlicher Verwaltungshelfer. Im Normalfall erlangt ZITiS dabei keine Kenntnis verfahrensbezogener Inhalte. Jedoch ist dies auch weiterhin rechtmäßig, wenn die Kenntnis verfahrensbezogener Inhalte für die Durchführung notwendig ist und die beauftragende Stelle dies so vorsieht, der Gedanke der Amtshilfe als Verwaltungsinstitution bestätigt dies.
Amtshilfen richten sich bei Anfragen von Landesbehörden nicht nach dem Errichtungserlass, sondern nach den allgemeinen rechtlichen Vorgaben zur Amtshilfe in Grundgesetz und Verwaltungsverfahrensgesetzen. Auch hier ist es Voraussetzung einer jeden Amtshilfe, dass der ersuchten Behörde die Ausführung einer Amtshilfehandlung rechtlich und tatsächlich möglich ist.

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)?

Zu 34:
Zunächst wird auf die Ausführungen zu Frage 33 verwiesen. ZITiS hat in 14 Fällen den Hochleistungsrechner genutzt, um im Rahmen von Amtshilfen für Landesbehörden als behördlicher Verwaltungshelfer zuzuarbeiten. Zu den zugrundeliegenden Ermittlungsverfahren liegen ZITiS keine Erkenntnisse vor. Darüber hinaus wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

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

Zu 35:
Die Frage wird so verstanden, dass die Fragesteller die Einschätzung der Bundesregierung zur Abgrenzung einer zulässigen von einer unzulässigen Amtshilfe anfragen. Nach Art. 35 Abs. 1 GG und entsprechenden verwaltungsverfahrensrechtlichen Vorschriften etwa in § 5 des Verwaltungsverfahrensgesetzes ist rechtlich vorgegebene Voraussetzung einer Amtshilfe ein nur ausnahmsweises, d. h. punktuelles, nicht aber regelmäßiges Unterstützen einer anderen Behörde. Wie es auch das Bundesverfassungsgericht ausführte, ist eine Amtshilfe immer eine Aushilfe im Einzelfall. Somit ist für ZITiS die Grenze zwischen Hilfeleistung in Einzelfällen und Ausnahmesituationen und einer regelmäßigen Unterstützung auch von Landespolizeien und Verfassungsschutzämtern nicht 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 dieser 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)?

Zu 36:
Die Bundesregierung kann diesen Sachverhalt bestätigen. Die von ZITiS gemeldete Sicherheitslücke war bereits im entsprechenden sicherheitstechnischen Umfeld bekannt.

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 um konkrete Nennung)?

Zu 37:
Es wird auf Vorbemerkung der Bundesregierung verwiesen.

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?*

Zu 38:
§ 4 Abs. 3 BSIG i. V. m § 4 Abs. 2 BSIG verpflichtet die Behörden des Bundes u. a. bereits zur Übermittlung von Informationen zu Schadprogrammen und Sicherheitslücken, soweit andere Vorschriften dem nicht entgegenstehen. Der Einführung einer Meldepflicht für alle Behörden und öffentlichen Stellen, d. h. auch für Behörden und öffentliche Stellen von Ländern und Kommunen, steht die Kompetenzverteilung des Grundgesetzes entgegen (vgl. Art 30 GG). Die Bundesregierung beabsichtigt nicht, diese zu verändern.

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?*

Zu 39 und 40:

Die Fragen 39 und 40 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Konzepte für ein Schwachstellenmanagement werden zum Beispiel in den USA, Niederlanden und Großbritannien diskutiert bzw. bereits teilweise oder in Gänze umgesetzt. Die Bundesregierung bewertet Prozesse anderer Staaten schon aufgrund der jeweils unterschiedlichen Rahmenbedingungen nicht. Die Bundesregierung setzt sich derzeit inhaltlich mit dieser Thematik auseinander. Da die Meinungsbildung innerhalb der Bundesregierung hierzu nicht abgeschlossen ist, kann zur Frage der Bewertung von Sicherheitslücken oder auch zu Rahmenbedingungen im Umgang mit Sicherheitslücken keine Aussage getroffen werden.

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 Entschlüsse-

lung“ 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)?

Zu 41:
Der Begriff „Staatstrojaner“ ist 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, ungeeignet, wie die Bundesregierung bereits im Rahmen der Beantwortung mehrerer Kleiner Anfragen, beispielsweise in der Bundestagsdrucksache 18/11261 zu Frage 13, Bundestagsdrucksache 19/1434 zu Frage 18 oder Bundestagsdrucksache 19/12465 zu Fragen 11 bis 11e dargestellt hat. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Zu 42:
Zunächst wird auf die Ausführungen der Bundesregierung zu dem Begriff „Staatstrojaner“ in der Antwort zu Frage 41 verwiesen. Im Übrigen wird auf den als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

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?

Zu 43:
Zunächst wird auf die Ausführungen der Bundesregierung zu dem Begriff „Staatstrojaner“ in der Antwort zu Frage 41 verwiesen. Die Quellen-Telekommunikationsüberwachung ist angesichts zunehmender Verschlüsselung eine für die Handlungsfähigkeit der Sicherheitsbehörden wichtige Fähigkeit. Vor dem Hintergrund der Stärkung einer Digitalen Souveränität ist daher eine krisenfeste Versorgungssicherheit anzustreben. Staatliche Eigenentwicklung ist ein unverzichtbarer Teil, um dies gewährleisten zu können, um die Abhängigkeiten von Herstellern und Dienstleistern aus dem Nicht-EU-Ausland zu verringern und um das Einhalten gesetzlicher Vorgaben und der korrespondierenden ethischen Werte sicherzustellen. ZITiS wird daher auf Basis seines Errichtungserlasses Kapazitäten erweitern, um für die Behörden des Bundes mit Sicherheitsaufgaben Forschungen und Entwicklungen auf dem Gebiet der Quellen-TKÜ anbieten zu können.
Damit die Sicherheitsbehörden nicht von den Ergebnissen des technologischen Fortschrittes abgekoppelt werden, muss darüber hinaus der Einsatz von Produkten aus globalen Lieferketten ebenfalls möglich sein. Um dies gesichert und selbstbestimmt tun zu können, baut ZITiS die Kompetenz auf, um die Behörden des Bundes mit Sicherheitsaufgaben auf diesem Gebiet beraten zu können und Produkte evaluieren zu können.

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)?

Zu 44:
Die ZITiS ist an keinem EU-Projekt im Sinne der Fragestellung beteiligt.

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)?

Zu 45
Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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 Messengerdienste wie Telegram zu verschaffen (bitte Projekte konkret aufschlüsseln)?

Zu: 46:
Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Zu 47:
a) Beim Fragegegenstand „Unterstützung bei der Technologievorausschau und -bewertung – 'Trendstudie'“ handelt es sich um kein Gutachten, sondern um eine umfassende Studie. Die Höhe des Beratungshonorars resultiert aus dem Aufwand, der mit der Erstellung einer Trendstudie verbunden ist. Die Honorarsumme in der Höhe von 225.329,48 Euro (Brutto) entspricht marktüblichen Preisen, die für die Erstellung vergleichbarer Untersuchungen anfallen.
b) Am 27. Mai 2020 wurde die Kooperationsvereinbarung geschlossen, die den Vertragsbeginn markiert.
c) Die Trendstudie sollte vertragsgemäß bis zum 11. Dezember 2020 abgeliefert werden. Aufgrund von Auswirkungen der Corona-Pandemie haben sich jedoch Verzögerungen ergeben.

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?

Zu 48:

a) Die nachfolgenden Rechtsgutachten wurden bei folgenden Vertragspartnern in Auftrag gegeben:
   - 2018: „Rechtsgutachten zur Aufgabenerfüllung der ZITiS“: Prof. Dr. Heinrich Amadeus Wolff;
   - 2019: „Erweiterung des erstellten Rechtsgutachtens zur Aufgabenerfüllung der ZITiS um die Fragestellung zur Aufnahme von ZITiS in die Sicherheitsüberprüfungsfeststellungsverordnung“: Prof. Dr. Heinrich Amadeus Wolff;
   - 2020: „Rechtsgutachten Suchdienst Darknet“: Prof. Dr. Jan-Henrik Dietrich;
   - 2020: „Unterstützung bei der Technologievorausschau und -bewertung – 'Trendstudie'“: Roland Berger GmbH;

b) Nachfolgend werden die wesentlichen Ergebnisse der Gutachten zusammengefasst:
   - 2018: „Rechtsgutachten zur Aufgabenerfüllung der ZITiS“:
     Das Rechtsgutachten zur Aufgabenerfüllung der ZITiS führt dazu aus, welche Rechtsnatur die ZITiS aufweist, welche konkreten Aufgaben der ministerielle Errichtungserlass für ZITiS vorsieht, wer die ZITiS wie beauftragen kann und wer nicht und wie sich die Fachaufsicht im Einzelnen darstellt, insbesondere in Ausprägung des Jahresarbeitsprogramms.
   - 2019: „Erweiterung des erstellten Rechtsgutachtens zur Aufgabenerfüllung der ZITiS um die Fragestellung zur Aufnahme von ZITiS in die Sicherheitsüberprüfungsfeststellungsverordnung“:
     Das Rechtsgutachten zur Erweiterung des erstellten Rechtsgutachtens zur Aufgabenerfüllung der ZITiS um die Fragestellung zur Aufnahme von ZITiS in die Sicherheitsüberprüfungsfeststellungsverordnung widmet sich der

Frage, ob und inwieweit die ZITiS aus rechtlicher Sicht in die Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) aufgenommen werden kann. Ergebnis des Gutachtens ist, dass u.a. aufgrund der Ähnlichkeit zur Forschungstätigkeit der in § 1 SÜFV aufgenommenen Behörden und des Sinns und Zwecks der Tätigkeit von ZITiS als Dienstleister für Nachrichtendienste die Möglichkeit bestünde, ZITiS in die Liste der Behörden gemäß § 1 SÜFV aufzunehmen.

- 2020: „Rechtsgutachten Suchdienst Darknet“:
  Das Rechtsgutachten Suchdienst Darknet befasst sich mit der Frage, ob und wie es der ZITiS möglich sei, einen Suchdienst für das Darknet im Auftrag seiner Kunden zu entwickeln. Das Rechtsgutachten stellt hierbei fest, dass die projektbezogene Tätigkeit von ZITiS in einem Bereich stattfinde, in dem das darauf bezogene Verfassungsrecht und einfache Recht in einer dynamischen Entwicklung begriffen sei.
  Die Befugnis zur projektbezogenen Forschungs- und Entwicklungstätigkeit von ZITiS könne unproblematisch auf deren Aufgabenzuweisung im Errichtungserlass gestützt werden, soweit Eingriffe in Grundrechte damit nicht verbunden sind.
  Das Rechtsgutachten berät auch dazu, welche verwaltungsorganisatorischen und rechtlichen Maßnahmen zur teilweisen Umsetzung des Projektes notwendig seien. Vorläufig solle ZITiS die projektbezogene Forschungs- und Entwicklungstätigkeit mit einer expliziten Beauftragung durch die Bedarfsträger BKA und BfV absichern.
- 2020: „Unterstützung bei der Technologievorausschau und -bewertung – 'Trendstudie'“: Die Studie soll bis Ende Januar 2021 fertiggestellt werden.

Eine Veröffentlichung der Gutachten „Rechtsgutachten zur Aufgabenerfüllung der ZITiS“, „Erweiterung des erstellten Rechtsgutachtens zur Aufgabenerfüllung der ZITiS um die Fragestellung zur Aufnahme von ZITiS in die Sicherheitsüberprüfungsfeststellungsverordnung“ und „Rechtsgutachten Suchdienst Darknet“ ist aufgrund der zugrundeliegenden Zusammenarbeit der ZITiS mit Sicherheitsbehörden nicht vorgesehen. Die Prüfung einer Veröffentlichung der Studie „Unterstützung bei der Technologievorausschau und -bewertung – 'Trendstudie'“ ist noch nicht abgeschlossen. Im Übrigen ergibt sich aus dem parlamentarischen Fragerecht grundsätzlich nur ein Anspruch gegen die Bundesregierung auf Beantwortung gestellter Fragen, was hier mit Zusammenfassung des Inhalts der Gutachten erfolgte, aber kein Recht auf Herausgabe von Dokumenten.