Deutscher Bundestag **Drucksache 21/2289**

21. Wahlperiode 16.10.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Donata Vogtschmidt, Clara Bünger, Desiree Becker, weiterer Abgeordneter und der Fraktion Die Linke – Drucksache 21/1697 –

Risiken für die IT-Sicherheit bei Online-Durchsuchung und Quellen-Telekommunikationsüberwachung („Staatstrojanern“)

Vorbemerkung der Fragesteller

Sowohl die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) als auch die Online-Durchsuchung sind Maßnahmen, die Sicherheitsbehörden ergreifen, um eine Fernüberwachung von Geräten der Zielperson zu ermöglichen. Dabei ist auch ein Zugriff auf verschlüsselte Inhalte möglich. Die Maßnahmen können durchgeführt werden, indem geheim gehaltene technische Schwachstellen auf Endgeräten ausgenutzt werden, beispielsweise um eine Spähsoftware einzubringen – sogenannte Staatstrojaner.

Der daraus resultierende hoheitliche Interessenskonflikt aus IT-Sicherheit und Schwächung derselben durch Ausnutzung von geheim gehaltenen IT-Schwachstellen wurde unter anderem vom Chaos Computer Club kritisiert (www.ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf). Das Problem verschärft sich durch die teilweise widersprüchlichen Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in diesem Kontext, weshalb immer wieder Forderungen nach mehr Unabhängigkeit und geänderten Aufgabenstellungen des BSI laut werden (https://link.springer.com/article/10.1365/s43439-024-00134-0). Hinzu kommen weitere Risiken wie beispielsweise die Nutzung von in Deutschland entwickelter Trojanersoftware auch in Staaten mit zweifelhafter Rechtsstaatlichkeit, teilweise sogar ohne Exportgenehmigung (https://netzpolitik.org/2023/unsere-strafanzeige-staatsanwaltschaft-klagt-manager-von-finfisher-an/), sowie Trojaner zur Ausspähung von Politikerinnen und Politikern und Journalistinnen und Journalisten auch innerhalb der europäischen Union (www.tagesschau.de/ausland/europa/pegasus-bericht-eu-100.html; https://netzpolitik.org/2023/staatstrojaner-wie-deutsche-an-der-spionagesoftware-predator-mitverdienen/; https://netzpolitik.org/2025/us-israelische-firma-paragon-neue-details-zu-spionage-angriff-mit-trojaner-graphite/). Die Reporter ohne Grenzen reichten im Jahr 2023 Verfassungsbeschwerde zum Artikel-10-Gesetz ein, da es sich mutmaßlich um eine zweifelhafte Rechtsgrundlage handelt, die derartige Trojanereinsätze durch deutsche Dienste erlaubt (www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/rsf-reicht-verfassungsbeschwerde-ein). Motive und Akteure hinter eingesetzten Staatstrojanern bleiben, sofern die Infektion überhaupt erkannt wurde, oft im Dunkeln. Bei der technisch anspruchsvollsten bisher bekannt gewordenen Ab-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 16. Oktober 2025 übermittelt.

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

hörmaßnahme „Operation Triangulation“ ist bis heute unbekannt, wer die Software entwickelt hat und aus welchen Motiven sie eingesetzt wurde (www.futurezone.de/digital-life/article515437/apple-hacker-angriff-experten.html).

Seitens der Bundesregierung gibt es bisher keine aktuellen Informationen, welche Staatstrojaner sie derzeit einsetzt oder beschafft hat. Allerdings ist im Koalitionsvertrag der amtierenden Bundesregierung von CDU, CSU und SPD eine Ausweitung des Einsatzes von Staatstrojanern festgehalten, etwa im Rahmen des derzeit in Novellierung befindlichen Bundespolizeigesetzes, während im August 2025 das Bundesverfassungsgericht die Rechtmäßigkeit von Trojanereinsätzen nur bei besonders schweren Straftaten bestätigte (www.spiegel.de/netzwelt/karlsruhe-bundesverfassungsgericht-schraenkt-staatliche-ueberwachung-mit-trojanern-ein-a-2018eac0-0292-40dd-8412-f1cbb49dffa6). Das Bundesamt für Justiz hat die Statistiken zur Telekommunikationsüberwachung und Online-Durchsuchung für das Jahr 2023 veröffentlicht (www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2025/20250805.html). Hinzu kommen von deutschen Geheimdiensten durchgeführte Quellen-TKÜ und Online-Durchsuchungen, worüber im Einzelnen nur die geheim tagende G10-Kommission und im Allgemeinen das Parlamentarische Kontrollgremium informiert ist, sowie Trojanereinsätze in Deutschland durch ausländische Geheimdienste, über die ebenfalls keine gesicherten Informationen öffentlich vorliegen.

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 die Fragen (6, 6a, 9, 9a und 12) nicht offen, die Fragen (6b, 7, 7a bis 7e, und 13b) auch nicht in eingestufter Form beantwortet werden können.

Im Einzelnen:

Die Antworten zu den Fragen 6, 6a, 9, 9a und 12 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 (Bundeskriminalamt (BKA), Bundespolizei (BPOL), Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und Zollkriminalamt – ZKA) und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden, 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.

Hinsichtlich der Fragen 6, 6a, 6b, 7, 7a, 7b, 7c, 7d, 7e und 13b ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass diese für die Nachrichtendienste des Bundes nicht beantwortet werden können. Gegenstand der Fragen sind solche Informationen, die in besonderem Maße das Staatswohl berühren und auch aufgrund der Restriktionen der Third-Party-Rule nicht veröffentlicht werden dürfen. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten zu Kooperationen der Nachrichtendienste mit Dritten, die besonders schützenswert sind, öffentlich bekannt werden. Diese Informationen sind geheimhaltungsbedürftig, weil sie sicherheitsrelevante Erkenntnisse enthalten, die unter der Maßgabe der vertraulichen Behandlung von Dritten an die Nachrichtendienste weitergeleitet wurden.

Darüber hinaus würde eine Bekanntgabe von Einzelheiten zu der im Rahmen der Aufgabenerfüllung genutzten Software weitgehende Rückschlüsse auf die technischen Fähigkeiten und unmittelbar auf die technische Ausstattung und das Aufklärungspotential der Nachrichtendienste des Bundes zulassen. Dadurch könnten die Fähigkeiten der Nachrichtendienste des Bundes, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden.

Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung der Nachrichtendienste des Bundes jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies betrifft insbesondere die Möglichkeiten zur Aufklärung nationaler und internationaler terroristischer Bestrebungen, bei denen derartige Kommunikationsmittel in besonderem Maße von den beobachteten Personen genutzt werden.

Selbst eine VS-Einstufung und Hinterlegung der Antwort in der Geheimschutzstelle des Deutschen Bundestages, würde der erheblichen Brisanz der Informationen im Hinblick auf die Bedeutung für die Aufgabenerfüllung der Nachrichtendienste nicht gerecht werden. Die angefragten Inhalte beschreiben Fähigkeiten und Arbeitsweisen der Nachrichtendienste so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bekannt gewordene Informationen, die nach den Regeln der Third-Party-Rule erlangt wurden, würden als Störung der wechselseitigen Vertrauensgrundlage gewertet werden. Die einzelnen Kooperationspartner arbeiten mit den Nachrichtendiensten nur unter der Voraussetzung zusammen, dass die konkrete Kooperation mit ihnen – auch nicht mittelbar – preisgegeben, sondern absolut vertraulich behandelt wird. Dies bedeutet, dass die geheimhaltungsbedürftigen Informationen zu und aus Kooperationen nicht außerhalb der Nachrichtendienste weitergegeben werden dürfen. Ein Bekanntwerden von Kooperationspartnern würde das Ansehen von deutschen Nachrichtendiensten und das Vertrauen in diese daher weltweit erheblich schädigen. Dementsprechend bestünde die ernstzunehmende Gefahr eines weitreichenden Wegfalls von Kooperationsmöglichkeiten nicht nur mit zivilen Firmen. Es wäre zudem zu befürchten, dass Kooperationspartner ihrerseits die Vertraulichkeit nicht oder nur noch eingeschränkt wahren würden. In der Konsequenz könnte es künftig zu einem Rückgang oder zum Wegfall zukünftiger Vertragspartner und in der Folge zu einem Wegfall der Erkenntnisgewinnung der deutschen Nachrichtendienste kommen. Dies hätte signifikante Informationslücken und negative Folgewirkungen für die Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland zur Folge. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zu-

rückstehen. Hier überwiegt daher ausnahmsweise das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht

Soweit die Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben BKA, BPOL und ZKA von den Fragestellungen betroffen sind, kann die Beantwortung aller Fragen mit Ausnahme der Fragen 2, 5, 6, 6a, 6b, 7, 7a, 7b, 7c, 7d, 7e, 9, 9a, 12 und 13b ebenfalls nicht und die Fragen 6, 6a, 9, 9a und 12 nicht vollumfänglich erfolgen.

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. Diese taktischen Einzelheiten umfassen insbesondere die hier von den Fragestellungen umfassten Methoden zur forensischen Sicherung und Analyse, Umgehung oder Entsperrung von Verschlüsselungen sowie das Einbringen von Software, darüber hinaus auch die Informationen über den konkreten operativen Einsatz entsprechender Software inklusive der Frage über etwaige Alternativen. Durch ein Bekanntwerden der genannten Methoden könnten die Fähigkeiten der Sicherheitsbehörden mit polizeilichen Aufgaben, Erkenntnisse im Wege der technischen Strafaufklärung 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 Gewinnung von Informationen durch eine IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr aber für die Aufgabenerfüllung 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 BKA – verankert im Grundgesetz (Artikel 73 Nummer 10 des Grundgesetzes – GG, Artikel 87 GG) und im Bundeskriminalamtgesetz (BKAG), BPOL (Artikel 87 GG sowie Bundespolizeigesetz – BPolG) und ZKA (Artikel 87 GG, Zollfahndungsdienstgesetz – ZFdG) – nicht mehr sachgerecht erfüllt werden könnten.

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 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 für diesen Teil der Fragen gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

1. Betreibt die Bundesregierung ein Schwachstellenmanagement im Sinne der Entscheidung des Bundesverfassungsgerichts vom 8. Juni 2021 (1 BvR 2771/18, Randnummer 34 ff.)?

Die Bundesregierung betreibt ein Schwachstellenmanagement zur Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.

Gemäß § 4 Absatz 2 bis 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) müssen grundsätzlich alle Bundesbehörden Informationen im Zusammenhang mit neu festgestellten Schwachstellen (Zero-Day-Schwachstellen), die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, an das BSI melden.

Gefundene Schwachstellen werden über das BSI dem betroffenen Hersteller gemeldet, damit dieser die Möglichkeit erhält, die Schwachstelle zu schließen. Das Verfahren zielt darauf ab, den durch eine mögliche Ausnutzung von Schwachstellen resultierenden Schaden zu minimieren.

Als bewährte Methode, sowohl national wie auch international wird dieser „Coordinated Vulnerability Diclosure“ (CVD) Prozess anerkannt.

a) Ist dieser Evaluationsprozess bereits gesetzlich verankert, und wenn ja, in welchen Normen?

Die Bundesregierung prüft, ob bezüglich dieser Prozesse infolge des Beschlusses des BVerfG vom 8. Juni 2021 – 1 BvR 2771/18 – ein Anpassungsbedarf besteht.

Schon heute sind die materiell-rechtlichen Vorgaben für Eingriffe in Grundrechte durch informationstechnische Überwachungsmaßnahmen, die ein Schwachstellenmanagement notwendig machen, in verschiedenen Gesetzen, etwa der Strafprozessordnung (StPO) geregelt. Für die Quellen-TKÜ und die Online-Durchsuchung zu Zwecken der Strafverfolgung gilt – neben dem allgemeinen Erfordernis der Verhältnismäßigkeit –, dass das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist (§ 100a Absatz 5 Satz 2, ggf. in Verbindung mit § 100b Absatz 4 StPO). Im Bereich der Gefahrenabwehr ergibt sich das gleiche Erfordernis für das BKA aus § 49 Absatz 2 Satz 2, ggf. in Verbindung mit § 51 Absatz 2 Satz 2 BKAG. Außerdem kann eine Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 (DSGVO) bzw. Folgenabschätzung nach § 67 des Bundesdatenschutzgesetzes (BDSG) erforderlich sein. Artikel 35 Absatz 7 Buchstabe c DSGVO verlangt u. a., dass die Folgenabschätzung „eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person“ enthalten muss. Auch bei Auslegung von § 67 BDSG ist zu berücksichtigen, dass nach Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 (JI-Richtlinie), dessen Umsetzung § 67 BDSG dient, auch den Rechten und berechtigten Interessen der betroffenen Person und sonstiger Betroffener Rechnung zu tragen ist.

b) Welche Kriterien liegen dieser Evaluation zugrunde?

Die Kriterien zur Evaluation der Schwachstellen basieren auf internen Prozessen der jeweils zuständigen Behörden.

c) Gibt es eine dazugehörige Verwaltungsvorschrift, und wenn ja, welche?

d) Ist der Prozess einheitlich für alle infrage kommenden Behörden geregelt, wenn nein, bitte auf Unterschiede eingehen?

Die Fragen 1c und 1d werden auf Grund ihres Sachzusammenhanges gemeinsam beantwortet.

Die Ausgestaltung der internen Prozesse und Verfahren richtet sich nach den jeweiligen gesetzlichen Aufgaben.

e) Inwiefern ist dieser Evaluationsprozess auch dann wirksam, wenn hinsichtlich der genutzten Schwachstellen direkt oder indirekt auf private Anbieter als Dienstleister zurückgegriffen wird?

Der Umgang mit Schwachstellen erfolgt nach den für die jeweilige Sicherheitsbehörde geltenden gesetzlichen Vorgaben.

2. Evaluiert die Bundesregierung in irgendeiner Form, in welchem Verhältnis das Offenhalten von IT-Schwachstellen zur Durchführung von Quellen-TKÜ und Online-Durchsuchung in Abwägung der tatsächlich erzielten Ermittlungserfolge (qualitativ und quantitativ) mit den Risiken für die allgemeine IT-Sicherheit steht, und wenn ja, welche Akteure sind in diesen Evaluationsprozess eingebunden, und welche Akteure erhalten Berichte darüber?

Eine Evaluation im Sinne der Fragestellung findet statt. Für diese Evaluierung gelten die im Beschluss des Bundesverfassungsgerichts vom 8. Juni 2021 (1BvR 2771/18) des Bundesverfassungsgerichts vom 8. Juni 2021 genannten Vorgaben.

Der Anordnung dieser Maßnahmen liegen Sachverhalte zugrunde, in denen ein Verdacht hinsichtlich einer schweren Straftat (Quellen-TKÜ) oder besonders schweren Straftat (Online-Durchsuchung) besteht oder in denen dringende Gefahren abzuwehren sind. Die Ermittlung der Umstände in diesen Fällen ist daher regelmäßig von wesentlicher Bedeutung.

3. Warum hat die Bundesregierung ihrem Gesetzentwurf zur nationalen Umsetzung der europäischen NIS2-Richtlinie nach (Bundesratsdrucksache 369/25) die Auffassung, dass das BSI keine Kenntnis darüber erhalten soll, wie viele und welche IT-Schwachstellen für Zwecke der Sicherheitsbehörden einschließlich der Geheimdienste geheim gehalten werden, und warum soll die Geheimhaltung von IT-Schwachstellen in den konkreten Einzelfällen jeweils nicht vom Einvernehmen mit dem BSI abhängig gemacht werden?

Der Gesetzentwurf der Bundesregierung zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung führt die bestehende Verpflichtung aller Bundesbehörden, Informationen im Zusammenhang mit neu festgestellten Schwachstellen (Zero-Day-Schwachstellen), die für die Erfüllung von Auf-

gaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, an das BSI zu melden, in § 43 Absatz 5 und 6 BSIG (neu) fort.

Im Übrigen wird auf die Antwort zu Frage 1 verwiesen

4. Welche Schlussfolgerungen zieht die Bundesregierung aus den in der Vorbemerkung der Fragesteller erwähnten diskutierten Vorschlägen hinsichtlich des BSI, die zu einer Beseitigung von Interessenskonflikten führen sollen, die zwischen dem Schutz der IT-Sicherheit und der Unterstützung von Sicherheitsbehörden möglicherweise auch zulasten der IT-Sicherheit bestehen, als da wären:

   a) vollständige Verschiebung von Aufgaben der Unterstützung von Sicherheitsbehörden zur Wahrung ihrer Aufgaben (beispielsweise gemäß § 3 Absatz 1 Nummer 13 des BSI-Gesetzes) an die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS),

   b) Festschreibung im BSI-Gesetz, dass das BSI unbeeindruckt von entgegenstehenden behördlichen Weisungen IT-Schwachstellen stets an die Hard- und Softwarehersteller beziehungsweise Entwickler-Communities meldet und deren schnellstmögliche Beseitigung stets anstrebt,

   c) Aufstellung des BSI als Informationssicherheitsbeauftragter des Bundes, unabhängig vom Beauftragten der Bundesregierung für Informationstechnik,

   d) Unterstellung des BSI unter das neu geschaffene Bundesministerium für Digitales und Staatsmodernisierung (BMDS), wenigstens hinsichtlich der Aufgaben zur Wahrung von IT-Sicherheit,

   e) Revision der seit 2023 geltenden Stellung der BSI-Präsidentin als politische Beamtin,

   f) Aufstellung des BSI als oberste Bundesbehörde,

   g) sonstige Maßnahmen, die aus Sicht der Bundesregierung zielführend erscheinen?

Die Bundesregierung äußert sich nicht zu hypothetischen Fragestellungen.

5. Wie viele Anträge auf Exportgenehmigung von Abhör- und Überwachungstechnik (beispielsweise Einzelausfuhrgenehmigungen für Dual-Use-Güter in den Güterlistenpositionen 4A005, 4D004, 4E001c, 5D001e) welcher juristischen Personen wurden mit Wirkung zu welchem Zeitpunkt seitens der Bundesregierung in der 19., 20. und 21. Wahlperiode genehmigt (auf das parlamentarische Informationsrecht diesbezüglich wird verwiesen gemäß Antwort auf die Schriftliche Frage 98 auf Bundestagsdrucksache 21/469), und welche dieser Anträge betreffen Technik, die sich auch zur Quellen-TKÜ oder zur Online-Durchsuchung eignet?

Seit der 19. Wahlperiode (24. Oktober 2017) bis zum Stichtag 22. September 2025 wurden insgesamt 199 Einzelvorgänge in den Güterlistenpositionen 4A005, 4D004, 4E001c, 5D001e mit Abhör- und Überwachungstechnik für endgültige Ausfuhren genehmigt, davon ein Vorgang, der für die Quellen-TKÜ oder Onlinedurchsuchung geeignet ist.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

6. Wie viel Geld hat die Bundesregierung jeweils in den Jahren seit 2015 aufgewendet für Beschaffung, Entwicklung und Betrieb einschließlich Wartung und Schulung für Technologie und Personal (bitte jeweils nach Jahren getrennt angeben), mit dem Ziel eines Einsatzes in der Quellen-TKÜ oder für Online-Durchsuchung?

   a) Wie viel Geld für derartige Zwecke ist in den aktuellen Entwürfen der Bundeshaushalte 2025 und 2026 für die Jahre 2025 und 2026 entsprechend vorgesehen?

Die Fragen 6 und 6a werden gemeinsam beantwortet.

Es wird auf die als „VS-Nur für den Dienstgebrauch“ eingestuften Antwortteile gemäß der Vorbemerkung verwiesen.* Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

   b) Wie schätzt die Bundesregierung Personal-, Kosten-, sowie Schulungs- und Wartungsaufwand der bisher genutzten Software für Quellen-TKÜ oder Online-Durchsuchung ein, gemessen einerseits an der erwartbaren Dauer der Einsatzfähigkeit und andererseits gemessen am bisherigen praktischen Ermittlungserfolg?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

7. Bei welchen Anbietern hat die Bundesregierung zu welchem Zeitpunkt Produkte zu den in Frage 6 genannten Zwecken seit dem Jahr 2015 beschafft (wenn keine Auskunft zu Beschaffungen für Geheimdienste möglich ist, bitte wenigstens bezogen auf Beschaffungen für Polizeien beantworten, so wie es in der Vergangenheit auch erfolgte (https://netzpolitik.org/2013/bestatigt-deutsche-behorden-haben-staatstrojaner-finfisher-fur-150-000-euro-gekauft/), und wenn keine öffentliche Antwort erfolgt, bitte begründen, warum dies in der Vergangenheit möglich war und jetzt nicht mehr)?

   a) In welchen Jahren hat die Bundesregierung welche Produkte dieser Anbieter für Ermittlungszwecke genutzt?

Die Fragen 7 und 7a werden gemeinsam beantwortet.

Bei den angefragten Ausgaben und Aufwendungen handelt es sich um geheimhaltungsbedürftige Angelegenheiten, deren Offenlegung erhebliche nachteilige Auswirkungen für die Sicherheit der Bundesrepublik Deutschland zur Folge haben könnte. Aus diesem Grund können auch keine Detailangaben zu Produkten, Vorgehensweisen und Anbietern gemacht werden. Für die Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen.

* Das Bundesministerium des Innern hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

b) Kann bei Trojanern der NSO Group, deren Einsatz das Bundeskriminalamt (BKA) im Jahr 2021 bestätigt hatte (https://www.tagesschau.de/investigativ/ndr-wdr/spionagesoftware-nso-bka-107.html), ausgeschlossen werden, dass bei Nutzung der Software anfallende Daten in einer Weise gespeichert werden, dass Dritte wie beispielsweise die NSO Group Zugriff darauf erlangen können (bitte hinsichtlich vertraglicher als auch faktischer beziehungsweise technischer Aspekte jeweils hinsichtlich von Metadaten und Inhaltsdaten beantworten), und Server in welchen Staaten sind in die Verarbeitung personenbezogener Daten eingebunden?

Das BKA verfügt über kommerzielle Software zur Durchführung von Maßnahmen zur informationstechnischen Überwachung und setzt diese entsprechend der rechtlichen Grundlagen ein. Die jeweilige Software wird erst nach einem umfangreichen Testverfahren und Feststellung der Konformität mit den rechtlichen Vorgaben sowie der „Standardisierenden Leistungsbeschreibung“ zum Einsatz freigegeben und in Abhängigkeit von der operativen Bedarfslage kontinuierlich weiterentwickelt. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

c) In welchen Jahren hat die Bundesregierung welche eigenentwickelten Werkzeuge zur informationstechnischen Überwachung genutzt?

Das BKA entwickelt eigenständig Werkzeuge zur informationstechnischen Überwachung und setzt diese entsprechend der rechtlichen Grundlagen ein. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

d) Welche aktuellen Informationen zur Eigenentwicklung derartiger Werkzeuge kann die Bundesregierung öffentlich geben?

e) Welche Informationen kann die Bundesregierung dazu geben, welche Wege derzeit genutzt werden, um erforderliche IT-Schwachstellen für eigenentwickelte Spähsoftware ausfindig zu machen (beispielsweise Schwarzmarkt für Exploits, eigene Forschung, Vereinbarungen mit Herstellern der Zielhardware bzw. Zielsoftware, Dienstleistungen durch Dritte)?

Die Fragen 7d und 7e werden gemeinsam beantwortet.

Zum Erhalt und Verbesserung der Fähigkeiten der Sicherheitsbehörden hinsichtlich Methoden und Lösungen im Bereich der Informationstechnischen Überwachung betreibt die ZITiS gemäß ihrem Auftrag auch eigene Forschung und Entwicklung. Hierzu findet auch ein fortlaufender Austausch mit anderen Sicherheitsbehörden statt.

Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

8. a) Wann wurde die „Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung“ (www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile&v=9) letztmalig auf erforderliche Aktualisierung geprüft, und welche Akteure werden in den Evaluierungsprozess einbezogen?

Eine umfassende Überarbeitung der Standardisierenden Leistungsbeschreibung (SLB) fand 2018 unter Einbindung aller relevanten Stellen statt. Die SLB konkretisiert die aus den rechtlichen Bestimmungen resultierenden Vorgaben und definiert Prozessabläufe für die Durchführung von Maßnahmen der informati-

onstechnischen Überwachung. Die in der Frage aufgeführte Version der SLB mit Stand 5. Oktober 2018 ist die aktuellste Version.

b) Welche Stellen außer den Sicherheitsbehörden selbst (beispielsweise das BSI, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Gerichte, Kontrollgremien) haben Einsicht und auch verbindliche Interventionsmöglichkeiten (welche?) hinsichtlich I) von erstellten Risikoanalysen; II) der Ergebnisse von Prüfungen vor einem zielsystemspezifischen Einsatz der Software; III) von Informationen seitens von Herstellern von genutzter Software über Sicherheitsvorfälle, erkannte Sicherheitsmängel oder andere Ereignisse, die die sichere, rechtmäßige und ordnungsgemäße Durchführung von Quellen-TKÜ- bzw. Online-Durchsuchungsmaßnahmen gefährden und IV) Dokumentation der Prozesse der Erkenntniserlangung während der verdeckten Ermittlungsverfahren, und wie oft sind diesen Stellen Dokumente dieser Art im Jahr 2024 übermittelt und deren Rückmeldung berücksichtigt worden, mit erheblichen Auswirkungen auf die Bewertung der Ergebnisse aus diesen Dokumenten beziehungsweise auf die Ermittlungsverfahren selbst?

Im Rahmen ihrer gesetzlichen Befugnisse können berechtigte Stellen Einsicht bezüglich der ihnen zustehenden Kompetenzen nehmen, um den rechtskonformen Einsatz überprüfen zu können.

9. Stimmt die Bundesregierung der Aussage zu, dass IT-Schwachstellen neben dem Zweck der Quellen-TKÜ und Online-Durchsuchung auch für ein lokales Auslesen elektronischer Speichermedien gemäß § 110 der Strafprozessordnung (StPO) zurückgehalten beziehungsweise zu Ermittlungszwecken genutzt werden?

Es wird auf die als „VS-Nur für den Dienstgebrauch“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.* Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

a) Wie oft fanden derartige lokale Zugriffe beziehungsweise Auswertungen von Daten auf Endgeräten in den Jahren 2023 und 2024 statt – gegebenenfalls auch auf anderen Rechtsgrundlagen (Aufenthaltsrecht)?

Es wird auf die als „VS-Nur für den Dienstgebrauch“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.* Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

b) Stimmt die Bundesregierung zu, dass beim Auslesen elektronischer Speichermedien gemäß § 110 StPO nicht nur ein lesender Zugriff erlangt wird, sondern der Eingriff derart ist, dass zumindest technisch auch eine Veränderung beispielsweise von Nachrichteninhalten auf dem Gerät möglich wird, und wenn ja, warum sollte dies erforderlich sein?

Die Datensichtung im Zuge der kriminaltechnischen Untersuchungen erfolgt mit lesendem Zugriff. Zur Sichtung elektronischer Speichermedien wird grundsätzlich eine gesicherte Kopie erstellt, sodass eine Veränderung ausgeschlossen werden kann.

* Das Bundesministerium des Innern hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

c) Wie erklärt die Bundesregierung, dass es trotz der richterlichen Kontrolle derartiger Maßnahmen belegtermaßen (https://freiheitsrechte.org/themen/freiheit-im-digitalen/handyauswertung) dazu kommt, dass die Polizei tiefgreifenden und manipulativen Eingriff in die Integrität des Zielsystems erlangt und dabei auch Kommunikationsinhalte und Daten einsieht und analysiert, die mit dem Anlass der Beschlagnahme nichts zu tun haben?

d) Wie soll die Rechtmäßigkeit derartiger Einsätze überhaupt sichergestellt sein, wenn während des Einsatzes und nach dem Einsatz gar keine richterliche Überprüfung des Vorgangs erfolgt?

e) Plant die Bundesregierung, die StPO dahin gehend zu präzisieren oder eine Spezialvorschrift zu schaffen, sodass ein derart invasiver Eingriff bei einem Tathergang wie im oben referenzierten Fall künftig zweifelsfrei unzulässig wird – auch hinsichtlich der Vereinbarkeit mit europäischem Recht (vgl. Verfassungsbeschwerde wegen Beschlagnahme und Datenzugriff auf Mobiltelefon vom 29. Juli 2025, S. 89, 90 https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Handydatenauslesung-Bamberg/29.07.2025-Verfassungsbeschwerde-Datenzugriff-Beschlagnahme-94-ff.-StPO.pdf)?

Die Fragen 9c bis 9e werden aufgrund ihres Sachzusammenhanges gemeinsam beantwortet.

Die Durchsuchung, die Durchsicht von elektronischen Speichermedien sowie die Sicherstellung oder Beschlagnahme von Daten richten sich nach den §§ 94, 98, 102, 105, 110 ff StPO.

Die Datenerhebung, -speicherung und -auswertung von nach § 94 StPO sichergestellten Daten muss im Einzelfall verhältnismäßig sein, hat sich am Zweck des Ermittlungsverfahrens und der Sicherung der Originalität des Beweismittels auszurichten. Die Beweiserheblichkeit der Daten begrenzt damit den jeweiligen Umfang der Ermittlungsmaßnahmen im Einzelfall. An diese Vorgaben sind die Strafverfolgungsbehörden gebunden.

Werden elektronische Speichermedien zur Durchsicht mitgenommen, können die betroffenen Personen nach § 110 Absatz 4 StPO in Verbindung mit § 98 Absatz 2 Satz 2 StPO jederzeit gerichtliche Entscheidung beantragen. Gegen die gerichtliche Entscheidung, oder wenn ein Gericht die vorläufige Sicherstellung zum Zwecke der Durchsicht auf Antrag der Staatsanwaltschaft entsprechend § 98 Absatz 2 Satz 1 StPO bereits bestätigt hat, können die betroffen Personen Beschwerde gemäß § 304 StPO einlegen.

Im Falle von schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen kommt je nach den Umständen des Einzelfalls zudem ein Beweisverwertungsverbot in Betracht, d. h. das Beweismittel darf im Strafurteil nicht gegen den Angeklagten oder die Angeklagte verwendet werden. Vor diesem Hintergrund ist eine Überarbeitung der gesetzlichen Regelungen nicht beabsichtigt

10. a) Wie schätzt die Bundesregierung anhand empirischer Erhebungen die praktische Wirksamkeit der richterlichen Kontrolle polizeilicher Maßnahmen zur Quellen-TKÜ, zur Online-Durchsuchung und zu Maßnahmen der Beschlagnahme und Analyse von Speichermedien ein, wie hoch ist jeweils die Rate richterlicher Einsprüche bzw. Zurückweisungen von Maßnahmen, und welche Möglichkeiten sieht die Bundesregierung, die Wirksamkeit richterlicher Kontrolle zu erhöhen?

b) Wie bewertet die Bundesregierung mit Blick auf einen lebendigen demokratischen Rechtsstaat die parlamentarischen Kontrollmöglichkeiten der genannten Maßnahmen jeweils mit Blick auf deren Einsatz durch Polizeien und durch die Geheimdienste, und hat sie für die 21. Wahlperiode Pläne, daran etwas zu ändern, und wenn ja, was?

Die Fragen 10a und 10b werden aufgrund ihres Sachzusammenhanges gemeinsam beantwortet.

Die Fragen greifen in den Kernbereich exekutiver Eigenverantwortung der Bunderegierung ein. Aus dem Grundsatz der Gewaltenteilung folgt ein Kernbereich exekutiver Eigenverantwortung, der einen auch parlamentarisch grundsätzlich nicht ausforschbaren Initiativ-, Beratungs- und Handlungsbereich einschließt. Die Kontrollkompetenz des Parlaments erstreckt sich grundsätzlich nur auf bereits abgeschlossene Vorgänge und umfasst nicht die Befugnis, in laufende Verhandlungen und Entscheidungsvorbereitungen einzugreifen (BVerfGE 124, 78 [121]; 137, 185 [234 f.]).

11. Welche Priorität ordnet die Bundesregierung der Quellen-TKÜ und Online-Durchsuchung beim verdeckten Auslesen Ende-zu-Ende-verschlüsselter Kommunikationsinhalte zu, verglichen mit lokaler Zugriffserlangung, Methoden des Client-Side-Scannings durch vom Anbieter eingebrachte Hintertüren oder Spähprogramme, Schwächen der verschlüsselten Datenübertragung, Social Engineering durch verdeckte Ermittler gegenüber Anbietern oder den Betroffenen selbst und weiteren Maßnahmen?

Die Frage nach der Priorisierung verschiedener verdeckter Ermittlungsmethoden, insbesondere im Kontext der Ende-zu-Ende verschlüsselten Kommunikation, betrifft hochsensible operative und rechtliche Abwägungen. Die Bundesregierung verfolgt hierbei einen technologisch neutralen und strikt an der Verhältnismäßigkeit orientierten Ansatz.

Die Bundesregierung setzt auf starke Verschlüsselung als Standard und lehnt generell die Forderungen nach Backdoors und technische Standards ab, die entweder direkt oder indirekt zu einer Schwächung von Ende-zu-Ende-Verschlüsselung führen.

12. Ist die Bundesregierung der Auffassung, dass das Ausnutzen von technischen IT-Schwachstellen derzeit die einzige Möglichkeit für Sicherheitsbehörden ist, auf Ende-zu-Ende-verschlüsselte Kommunikationsinhalte zuzugreifen, und wenn nein, warum wird es dennoch als erforderlich angesehen, technische IT-Schwachstellen für diese Zwecke zu nutzen?

Eine Ende-zu-Ende Verschlüsselung dient dem Zweck die Kommunikation zwischen zwei Kommunikationsteilnehmern nur für diese lesbar zu machen. In diesen Fällen sind für eine Telekommunikationsüberwachung die Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung unerlässlich. Darüber hinaus wird auf die „VS-Nur für den Dienstgebrauch“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.*

* Das Bundesministerium des Innern hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

13. a) Entstehen nach Ansicht der Bundesregierung durch das Zurückhalten von IT-Schwachstellen, die Entwicklung von Staatstrojanern und das Schwächen von Verschlüsselung auch IT-Sicherheitsrisiken für die Sicherheitsbehörden selbst, und wenn ja, warum wird dieser Weg dennoch beschritten, und welche Maßnahmen ergreift die Bundesregierung, um ihre Sicherheitsbehörden vor diesen Risiken der Kompromittierung zu schützen?

Hinsichtlich der Maßnahmen zum Schutz der Sicherheitsbehörden wird auf die einschlägigen Prozesse und Regelungen zur IT-Sicherheit verwiesen, die unter der Federführung des BSI zusammengefasst sind.

Eine mögliche Nutzung von Schwachstellen erfolgt unter Berücksichtigung der im Beschluss des Bundesverfassungsgerichts vom 8. Juni 2021 (1 BvR 2771/18) genannten Vorgaben.

b) Nutzt die Bundesregierung in Sicherheitsbehörden oder im Militär spezielle Analysewerkzeuge, um mögliche Infektionen mit Spähsoftware, unsichere Verbindungen oder anderweitig kompromittierte Kommunikation festzustellen, und warum werden diese Werkzeuge nicht als Open-Source-Software öffentlich zum Schutz der Allgemeinheit zur Verfügung gestellt?

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

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.bundesanzeiger-verlag.de
ISSN 0722-8333