Deutscher Bundestag **Drucksache 21/1697**

21. Wahlperiode 17.09.2025

Kleine Anfrage

der Abgeordneten Donata Vogtschmidt, Clara Bünger, Desiree Becker, Anne-Mieke Bremer, Katrin Fey, Ates Gürpinar, Dr. Gregor Gysi, Luke Hoß, Ferat Koçak, Jan Köstering, Sonja Lemke, Bodo Ramelow, David Schliesing, Aaron Valent, Christin Willnat und der Fraktion Die Linke

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

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 Abhörmaßnahme „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.

Wir fragen die Bundesregierung:

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

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

   b) Welche Kriterien liegen dieser Evaluation zugrunde?

   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?

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

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?

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?

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?

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?

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?

   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?

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?

   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?

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

   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)?

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?

   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?

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?

   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)?

   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?

   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)?

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?

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?

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?

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?

    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?

Berlin, den 10. September 2025

Heidi Reichinnek, Sören Pellmann und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333