Deutscher Bundestag **Drucksache 21/4630**

21. Wahlperiode 11.03.2026

Kleine Anfrage

der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Martin Hess, Sascha Lensing und der Fraktion der AfD

Maßnahmen der Bundesregierung zur Verhinderung eines Datenabflusses über Telekommunikationskomponenten des Herstellers Huawei

Die Sicherheit und Integrität öffentlicher Telekommunikationsnetze sind eine zentrale Voraussetzung für die Funktionsfähigkeit des Staates, für den Schutz personenbezogener Daten sowie für die Resilienz kritischer Infrastrukturen. Insbesondere Mobilfunknetze der fünften Generation (5G) sind aufgrund ihrer Rolle für Verwaltung, Wirtschaft, Sicherheitsbehörden und zunehmend auch für industrielle Steuerungsprozesse sicherheitspolitisch besonders bedeutsam. Der Gesetzgeber hat hierzu im Telekommunikationsgesetz (TKG) spezielle Vorgaben für Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial geschaffen; dazu gehört insbesondere die Pflicht, kritische Komponenten vor dem erstmaligen Einsatz zertifizieren zu lassen und für kritische Komponenten zusätzliche Anforderungen einschließlich Herstellererklärungen zu erfüllen (www.gesetze-im-internet.de/tkg_2021/__165.html).

Ergänzend konkretisieren technische Regelwerke des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Nachweiserbringung und Zertifizierungswege für kritische Komponenten in öffentlichen Kommunikationsnetzen, etwa die Technische Richtlinie TR-03163 „Sicherheit in TK-Infrastrukturen“ (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03163/BSI-TR-03163.pdf?__blob=publicationFile&v=14).

Auch die Bundesnetzagentur veröffentlicht hierfür einschlägige Konkretisierungen, darunter eine „Liste der kritischen Funktionen“, die für die Einordnung von Komponenten und Risiken maßgeblich ist (www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/_DL/ListekritischeFunktionen.pdf?__blob=publicationFile&v=1), sowie den Katalog von Sicherheitsanforderungen nach dem TKG (www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/_DL/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=1).

Vor diesem regulatorischen Hintergrund wird seit Jahren öffentlich und parlamentarisch diskutiert, wie Risiken von Abhängigkeiten und möglichen Sicherheitslücken bei Ausrüstern in 5G-Netzen begrenzt werden können. Die Fraktion der AfD hat diese Debatte seit der 19. Wahlperiode mit Initiativen begleitet und dabei auf die Notwendigkeit eines konsequenten Schutzes kritischer 5G-Infrastruktur hingewiesen. Beispielhaft wird auf den Antrag „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ auf Bundesdrucksache 19/7723 verwiesen sowie auf die Kleine Anfrage „Möglicher Ausschluss

von Huawei beim Aufbau des deutschen 5G-Netzwerkes“ auf Bundestagsdrucksache 19/8650.

Zudem wurde in der gegenwärtigen Wahlperiode ein Antrag der Fraktion der Fraktion der AfD zur Zuständigkeitsausgestaltung des neuen Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) auf Bundesdrucksache 21/3316 eingebracht, was in den Augen der Fragesteller die Relevanz einer klaren Verantwortungszuordnung auch für Fragen der Netz- und Datensicherheit unterstreicht.

Nach Angaben der Bundesregierung hat das Bundesministerium des Innern (BMI) Betreiber öffentlicher 5G-Mobilfunknetze bereits 2023 aufgefordert, alle in den jeweiligen Netzen im Einsatz befindlichen kritischen Komponenten der Hersteller Huawei und ZTE mitzuteilen und nach einer vorgegebenen Systematik aufzulisten (www.bundestag.de/presse/hib/kurzmeldungen-951412?utm_source=chatgpt.com). Im Jahr 2024 teilte das BMI ferner mit, dass in 5G-Kernnetzen bis spätestens Ende 2026 keine Komponenten von Huawei und ZTE mehr eingesetzt werden dürfen und weitere Schritte auch Zugangs- und Managementbereiche betreffen sollen (www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/5g.html).

Aus Sicht der Fragesteller ist dabei entscheidend, welche technischen, organisatorischen und rechtlichen Maßnahmen die Bundesregierung konkret ergriffen hat und ergreift, um einen Datenabfluss oder unautorisierte Zugriffe über Komponenten bestimmter Hersteller in öffentlichen Kommunikationsnetzen auszuschließen bzw. bestmöglich zu verhindern, wie die Umsetzung überwacht wird und welche Rolle hierbei das BMDS spielt.

Wir fragen die Bundesregierung:

1. Auf welche konkreten Rechtsgrundlagen stützt die Bundesregierung die im Juli 2024 vom BMI kommunizierten Maßnahmen, wonach in 5G-Kernnetzen bis spätestens Ende 2026 keine Komponenten von Huawei und ZTE mehr eingesetzt werden dürfen, und in welcher Rechtsform wurden diese Maßnahmen gegenüber den Netzbetreibern verbindlich gemacht?
2. Welche Rolle und Zuständigkeit kommen dem Bundesministerium für Digitales und Staatsmodernisierung (BMDS) bei der strategischen Steuerung, Koordinierung und Kontrolle dieser Maßnahmen zu, und welche weiteren Bundesministerien sind in welcher Form beteiligt?
3. Welche Arbeitsdefinition von „Komponenten“ und „kritischen Komponenten“ legt die Bundesregierung in diesem Zusammenhang zugrunde, und wie grenzt sie diese Definitionen gegenüber den Begrifflichkeiten des TKG, insbesondere § 165 TKG, ab?
4. Welche konkreten Netzbereiche sind von den bis 2026 bzw. den weitergehenden Maßnahmen bis 2029 erfasst, und welche Netzbereiche sind nach aktuellem Stand ausdrücklich nicht erfasst (bitte getrennt nach 5G-Kernnetz, 5G-Zugangsnetz bzw. Radio Access Network, Transport- bzw. Backhaul, Netzmanagement- bzw. Orchestrierungs- und Betriebsunterstützungssystemen angeben)?
5. Welche Betreiber öffentlicher 5G-Mobilfunknetze wurden nach Kenntnis der Bundesregierung aufgrund der Aufforderung vom 6. März 2023 zur Meldung kritischer Komponenten zur Übermittlung welcher Daten verpflichtet, und haben alle Betreiber vollständig und fristgerecht geantwortet (bitte Betreiber nennen, soweit zulässig, andernfalls nachvollziehbar anonymisiert darstellen)?

6. Welche „kritischen Funktionen“ im Sinne der Veröffentlichungen der Bundesnetzagentur waren nach Kenntnis der Bundesregierung zum Zeitpunkt der Datenerhebung bzw. der Entscheidung in deutschen 5G-Netzen durch Komponenten von Huawei abgedeckt (bitte nach Funktionskategorie aufschlüsseln)?
7. Welche Zertifizierungs- und Nachweispflichten nach § 165 TKG sowie nach der BSI-TR-03163 wurden nach Kenntnis der Bundesregierung für Huawei-Komponenten in öffentlichen 5G-Netzen bereits erfüllt, und welche noch nicht (bitte jeweils nach Funktionsklasse bzw. Komponentenkategorie aufschlüsseln)?
8. Welche Prüf- und Kontrollmechanismen (z. B. Vor-Ort-Prüfungen, Dokumentenprüfungen, Penetrationstests, Code-Review-Ansätze, Zertifizierungsnachweise, Auditpflichten) setzt die Bundesregierung über das BMI, das BSI und/oder weitere Bundesbehörden ein, um einen Abfluss von Daten oder unautorisierte Zugriffe über Netzkomponenten auszuschließen bzw. bestmöglich zu verhindern (bitte Zuständigkeiten und Prüffrequenzen benennen)?
9. Welche Erkenntnisse liegen der Bundesregierung zu sicherheitsrelevanten Vorfällen, Schwachstellenmeldungen oder sonstigen Ereignissen mit Bezug zu Huawei-Komponenten in deutschen öffentlichen Mobilfunknetzen vor, die eine potenzielle Vertraulichkeitsverletzung (Datenabfluss) oder Integritätsverletzung nahelegen (bitte Anzahl, Zeitraum, Klassifizierung und zuständige Meldestellen angeben, soweit möglich)?
10. Welche Vorgaben macht die Bundesregierung den Netzbetreibern hinsichtlich der Behandlung von Software- bzw. Firmware-Updates für sicherheitsrelevante Netzfunktionen, und inwieweit werden Updates für als kritisch eingestufte Komponenten vor Einspielung geprüft oder zertifiziert (bitte die einschlägigen Regelwerke, Zuständigkeiten und Prozesse benennen)?
11. Welche Maßnahmen hat die Bundesregierung ggf. ergriffen, um sicherzustellen, dass in Bundesnetzen oder bundesnahen Netzinfrastrukturen (z. B. Netze von Bundesbehörden oder bundeseigenen Unternehmen) kein Einsatz von Huawei-Komponenten erfolgt, soweit dies sicherheitsrelevant ist, und welche Bestandsaufnahmen liegen hierzu vor (bitte nach Kenntnisstand der Bundesregierung aufschlüsseln)?
12. Welche Auswirkungen auf Kosten, Netzverfügbarkeit und Zeitpläne erwartet die Bundesregierung durch den Austausch der betroffenen Komponenten, und welche Vorkehrungen hat sie getroffen, um zu verhindern, dass daraus mittelbar finanzielle Belastungen des Bundes entstehen (bitte nach Kenntnis der Bundesregierung etwaige Szenarien, Vorsorgeinstrumente und Haushaltsvorsorge darstellen)?
13. Inwieweit bezieht die Bundesregierung bei ihrer Risikobewertung und Maßnahmenplanung die EU-Vorgaben bzw. Empfehlungen zur 5G-Sicherheit (EU-Toolbox) ein?

14. Welche Maßnahmen ergreift die Bundesregierung, um auch bei Netzen oder IT-Infrastrukturen im Zuständigkeitsbereich der Länder und Kommunen, soweit diese an bundesrelevante Kommunikations- oder Verwaltungsprozesse angebunden sind, Risiken durch den Einsatz potenziell kritischer Hersteller zu minimieren, und welche Erkenntnisse liegen ihr hierzu nach Kenntnis der Bundesregierung vor?

Berlin, den 9. März 2026

Dr. Alice Weidel, Tino Chrupalla 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