Deutscher Bundestag **Drucksache 21/5446**

21. Wahlperiode 16.04.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/5202 –

Resilienz deutscher BOS-Netze

Vorbemerkung der Fragesteller

In Zeiten zunehmender globaler Krisenlagen – seien es Cyberangriffe, geopolitische Spannungen, terroristische Bedrohungen oder großflächige Ausfälle kritischer Infrastrukturen – gewinnt die Frage der Resilienz der Kommunikationsnetze der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Deutschland existenzielle Bedeutung. Der sichere, störungsfreie und souveräne Betrieb des BOS-Digitalfunknetzes ist mehr als ein technisches Detail: Er ist Grundlage für jede staatliche Handlungsfähigkeit in Krisen- und Katastrophenfällen.

Das BOS-Digitalfunknetz besteht, laut offiziellen Angaben, aus vielen verschiedenen Komponenten (Basisstationen, Vermittlungsstellen, Richtfunkverbindungen, Endgeräte etc.) und wird technisch strukturiert betrieben. Die Steuerung und Koordination obliegen der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS; www.bdbos.bund.de/DE/Aufgaben/DigitalfunkBOS/DigitalfunkBOSimUeberblick/digitalfunkbosimueberblick_node.html).

Ein effizientes BOS-Netz verlangt nach Ansicht der Fragesteller nicht nur hohe Verfügbarkeit im Normalbetrieb, sondern vor allem Robustheit gegen Störungen, Ausfälle und feindliche Eingriffe – etwa bei längerem Stromausfall, Ausfall kommerzieller Netze, bei Cyberangriffen oder im Rahmen hybrider Bedrohungslagen. Dies betrifft Aspekte wie Redundanz, Abhörsicherheit, Verfügbarkeit auch bei überlasteter Infrastruktur oder sabotierten Leitungen sowie die Kontrolle über sämtliche eingesetzte Komponenten und deren Herkunft. In einem sicherheitssensiblen Umfeld darf nach Auffassung der Fragesteller keine Abhängigkeit von ausländischen bzw. fremdkontrollierten Komponenten bestehen, die im Krisenfall zur Achillesferse werden könnten.

Vor dem Hintergrund der gegenwärtigen sicherheitspolitischen Herausforderungen sowie der zunehmend dringlichen Notwendigkeit staatlicher Souveränität im Bereich kritischer Kommunikationsinfrastrukturen ist es in den Augen der Fragesteller unabdingbar, eine vollständige Transparenz über Bestand, Herkunft und Widerstandsfähigkeit sämtlicher Komponenten des BOS-Digitalfunknetzes herzustellen. Dabei bedarf es nach Ansicht der Fragesteller insbesondere einer präzisen Aufschlüsselung darüber, in welchem Umfang Hardware- und Softwarekomponenten im Einsatz sind, die von ausländischen Her-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 16. April 2026 übermittelt.

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

stellern stammen und somit potenziell Einflussnahmen durch Drittstaaten oder wirtschaftspolitischen Sanktionen ausgesetzt sein könnten. Ebenso stellt sich ihnen die Frage nach dem aktuellen Stand der geplanten Modernisierung und des Ausbaus des BOS-Netzes hin zu einer breitbandigen, datenfähigen Infrastruktur, wie sie etwa im Frequenzbereich zwischen 470 und 694 Megahertz (MHz) in verschiedenen Fachkonzepten gefordert wird.

Darüber hinaus muss nach Ansicht der Fragesteller offengelegt werden, welche konkreten Maßnahmen seitens des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) bzw. durch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben bislang getroffen wurden oder künftig vorgesehen sind, um sicherzustellen, dass sämtliche Aspekte der BOS-Kommunikationsinfrastruktur dauerhaft unter nationaler bzw. staatlicher Kontrolle verbleiben – insbesondere im Hinblick auf sensible Belange der nationalen Sicherheit und des Abhörschutzes. Schließlich ist für sie auch zu klären, wie im Krisenfall, etwa bei einem großflächigen Ausfall kommerzieller Netzinfrastrukturen oder bei längerem Stromausfall, die Betriebsfähigkeit des Netzes gewährleistet werden soll – sei es durch technische Redundanzen, durch Notstromversorgung, alternative Kommunikationswege oder durch vordefinierte Rückfalloptionen.

1. Welche Komponenten (Hardware und Software) werden nach Kenntnis der Bundesregierung aktuell im BOS-Digitalfunknetz eingesetzt, die von ausländischen Herstellern stammen (bitte nach Herstellerland, Stückzahl und Funktion, also Basisstationen, Vermittlungsstellen, Endgeräte, Richtfunk, Verschlüsselung, Leitsoftware etc., aufschlüsseln)?

Es werden ca. 5 000 Basisstationen und ca. 60 Vermittlungsstellen eines finnischen Herstellers eingesetzt.

Es werden insgesamt ca. 1 300 000 Endgeräte eines englischen, eines US-amerikanischen sowie eines niederländischen Herstellers eingesetzt.

2. Welche Richtlinien bzw. Beschaffungs- und Zulassungsprozesse existieren beim BMDS bzw. bei der BDBOS, um sicherzustellen, dass keine sicherheitskritischen BOS-Netzkomponenten ausländischer Herkunft eingebunden werden bzw. wenn sie eingebunden sind, wie deren Unabhängigkeit und Vertrauenswürdigkeit geprüft werden?

Es werden die einschlägigen Richtlinien des BSI-IT-Grundschutzes angewendet.

3. In welchem Umfang plant die Bundesregierung ggf., das bisher schmalbandig ausgelegte BOS-Netz durch ein breitbandiges, datenfähiges Netz zu erweitern (z. B. Nutzung von UHF-Frequenzen [UHF = Ultra High Frequency] 470 bis 694 MHz), um moderne Krisen- und Verteidigungslagen abzudecken (bitte den Zeitplan, die finanziellen Mittel und die involvierten Behörden bzw. Stellen angeben)?

Bund und Länder sind sich im Grundsatz einig, dass die gestiegenen und veränderten Nutzeranforderungen die zeitnahe Weiterentwicklung des bisherigen TETRA-Digitalfunks BOS zu einer mobilen breitbandigen einsatzkritischen Kommunikation erfordern. Für den Bund ist ein resilienter Breitbandfunk auf dem Stand der Technik essentiell, um die einsatzkritische Sprachkommunikation der BOS des Bundes langfristig zu sichern und zugleich um eine ebenfalls einsatzkritische Datenkommunikation funktional zu erweitern.

Für den Einstieg in den Breitbandfunk sind im Bundeshaushalt 2026 einschließlich der geltenden Finanzplanung insgesamt knapp 450 Mio. Euro (verteilt auf 2026: 89,2 Mio. Euro, 2027: 100 Mio. Euro, 2028: 110 Mio. Euro und 2029: 150 Mio. Euro) vorgesehen. Der Breitbandfunk soll im Zusammenwirken mit den Ländern bis zum Jahr 2030 errichtet werden. Die Nutzung eigener Frequenzen aus dem UHF-Band 470-694 MHz ist für die ersten Umsetzungsstufen nicht vorgesehen, ist im weiteren Programmverlauf gleichwohl berücksichtigt.

4. Wie wird die Resilienz des BOS-Netzes sichergestellt für den Fall eines großflächigen Strom-, Internet- oder Netzausfalls, insbesondere in Bezug auf Notstromversorgung, redundante Übertragungspfade (z. B. Richtfunk, Satellit, terrestrisch unabhängige Netze) sowie Aufrechterhaltung der Kommunikation auch bei Ausfall kommerzieller Netzinfrastruktur?

Ein Beauskunften der hier infragestehenden Informationen, kann aufgrund entgegenstehender überwiegender Belange des Staatswohls nur eingestuft erfolgen. Durch eine offene Auskunft darüber, welche Resilienz, Notfall und Rückfallebenen konkret im Digitalfunk BOS vorgesehen sind, wären Rückschlüsse auf die konkreten technischen Schutzmechanismen des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben möglich. Durch eine offene Auskunft über den aktuellen Wissensstand könnten Extremisten oder staatliche Akteure Angriffsvektoren und -strategien entwickeln und dadurch die Funktionsfähigkeit des Digitalfunks und damit die Aufgabenerfüllung der Behörden mit Sicherheitsaufgaben gefährden oder letztere sogar unmöglich machen. Dies würde einen Nachteil für die Interessen der Bundesrepublik Deutschland bedeuten. Eine offene Beantwortung der Frage ist daher nicht möglich und wird gesondert als „VS-Nur für den Dienstgebrauch“ eingestufte Anlage* übersendet.

5. Ist der Bundesregierung bekannt, ob Teile der BOS-Netzinfrastruktur durch ausländische Dienstleister oder Unternehmen ausgelagert, gewartet oder betrieben werden, wenn ja, um welche Unternehmen handelt es sich, mit Sitz in welchem Land, und was genau umfasst der jeweilige Auftrag?

Die für den Betrieb des Digitalfunks beauftragten Dienstleister sowie deren Unterauftragnehmer haben ihren Sitz ausschließlich in Deutschland.

6. Plant die Bundesregierung den Aufbau einer souveränen und vollständig deutschen BOS-Kommunikationsinfrastruktur, um Abhängigkeiten von ausländischer Hardware bzw. Software zu reduzieren, insbesondere durch Nutzung nationaler Hersteller, und wenn ja, welche konkreten Maßnahmen plant die Bundesregierung, diesbezüglich zu ergreifen bzw. zu setzen?

Die BDBOS betreibt mit dem TETRA-Digitalfunknetz eine vollständig eigenbeherrschte BOS-Kommunikationsinfrastruktur. Sie setzt für die TETRA-Systemtechnik ausschließlich auf europäische Lieferanten. Diese Strategie wird auch beim Aufbau des Digitalfunks der nächsten Generation verfolgt.

* 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.

7. Wie wird nach Kenntnis der Bundesregierung die Sicherheit der Datenkommunikation und Sprachkommunikation gewährleistet – insbesondere gegen Abhören, Manipulation oder Cyberangriffe –, und wie wird die Herkunft und Integrität der eingesetzten Verschlüsselungs- und Authentifizierungssoftware geprüft und dokumentiert?

Für den Digitalfunk BOS werden die Vorgaben aus dem BSI-IT-Grundschutz mit einem hohen Schutzbedarf im Betrieb umgesetzt. Die Sicherheit der Daten- und Sprachkommunikation wird durch Verwendung der von der ETSI standardisierten Luftschnittstellenverschlüsselung sichergestellt. Zudem kommt eine vom BSI entwickelte Ende-zu-Ende-Verschlüsselung zum Einsatz. Herkunft und Integrität der Software werden im Einklang mit den einschlägigen Richtlinien des BSI-IT-Grundschutzes geprüft und dokumentiert.

8. Liegt der Bundesregierung eine Risikoanalyse vor, die untersucht, wie im Falle von geopolitisch motivierten Sanktionen gegen Herstellerländer oder in Krisenlagen die Einsatzfähigkeit des BOS-Netzes beeinträchtigt werden könnte, und wenn ja, mit welchem Ergebnis?

An der Digitalfunk-Infrastruktur sind ausschließlich europäische Hersteller beteiligt. Geopolitisch motivierte Sanktionen gegen deren Länder können kurzfristig keine Auswirkungen auf die Einsatzfähigkeit des BOS-Netzes entfalten.

Die Einsatzfähigkeit des BOS-Netzes in Krisenlagen wird durch ein professionelles Notfallmanagement gemäß BSI-Standard sichergestellt.

9. Wird durch das BMDS bzw. die BDBOS ein Konzept für „Redundante Rückfallkommunikation“ verfolgt, etwa über satellitengestützte Netze, unabhängige Richtfunk-Netze oder andere stabile Kommunikationswege, und wenn ja, wie sieht dieses Konzept im Detail aus (Technik, Umfang, Zeitplan)?

Grundsätzlich sind die Basisstationen des TETRA-basierten Digitalfunks auf Leitungen und Richtfunkverbindungen abgestützt. Für mobile Basisstationen stehen ergänzend satellitenbasierte Anbindungen zur Verfügung. Für den Digitalfunk der nächsten Generation sind redundante satellitengestützte Rückfallebenen in der Planung vorgesehen.

10. Wurde nach Kenntnis der Bundesregierung in den letzten fünf Jahren geprüft, ob Teile der BOS-Netzkomponenten (Endgeräte, Basisstationen oder Software) von Herstellern stammen, die auf der „kritischen Infrastruktur“-Beobachtungsliste stehen, und wenn ja, welche Konsequenzen wurden ggf. gezogen?

Eine „kritische Infrastruktur“-Beobachtungsliste ist nicht bekannt. Im Übrigen ist die BDBOS als Betreiber des Digitalfunk-BOS kein Betreiber einer kritischen Anlage im Sinne des BSIG.

11. Welche Haushaltsmittel wurden in den letzten fünf Jahren vom Bund bzw. über die zuständigen Bundesministerien für den Ausbau, die Modernisierung und die Sicherung des BOS-Netzes bereitgestellt (bitte getrennt nach den Bereichen Basisstationen, Vermittlungsstellen, Endgeräte, Netzsicherheit, Verschlüsselung, Redundanz und Rückfallkommunikation ausweisen)?

Eine detaillierte Beantwortung ist nicht möglich. Die BDBOS erhält zweckgebundene Zuschüsse aus dem Bundeshaushalt. Diese decken den Bundesanteil am Gesamtfinanzierungsbedarf aus der Umsetzung des bestehenden Verwaltungsabkommens entsprechend der dort vereinbarten Finanzierungssachverhalte. Eine detaillierte Aufschlüsselung auf einzelne Ausgabepositionen ist auf dieser Ebene nicht vorgesehen.

Es wird daher hilfsweise eine Auswertung des Wirtschaftsplans der BDBOS zur Verfügung gestellt. Die nachstehend ausgewiesenen Werte enthalten IST-Ausgaben der BDBOS, die gleichermaßen die Bereiche Netzsicherheit, Verschlüsselung, Redundanz, Rückfallkommunikation sowie Endgeräte umfassen. Eine detailliertere Aufschlüsselung ist nicht möglich. Die im Jahresvergleich zunehmenden IST-Ausgaben sind durch die seit dem Jahr 2021 in aufwachsenden Modernisierungsmaßnahmen des Digitalfunknetzes begründet.

Anteil Bund in TEUR	**2021**	**2022**	**2023**	**2024**	**2025**
Vermittlungsstellen	160 103	233 607	279 290	299 745	345 201
Basisstationen	7 491	8 842	13 091	20 541	32 795
Summe	167 594	242 449	292 381	320 286	377 996

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