Deutscher Bundestag **Drucksache 21/5202**

21. Wahlperiode 07.04.2026

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

Resilienz deutscher BOS-Netze

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 Herstellern 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.

Wir fragen die Bundesregierung:

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)?
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?
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)?
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?
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?
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?
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?

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?
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)?
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?
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)?

Berlin, den 26. 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