

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Benjamin Strasser, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/3955 –

Digitalfunk und Einsatzkommunikation

Vorbemerkung der Fragesteller

Mit dem Inkrafttreten des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der BOS im Jahr 2006 wurde in der Bundesrepublik Deutschland der Grundstein eines bundesweiten, einheitlichen Digitalfunknetzes für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) gelegt. Zehn Jahre später – im Jahr 2016 – ging der Digitalfunk BOS nach Integration des letzten Netzabschnitts bundesweit in Betrieb. Seitdem besteht die Möglichkeit, die Funkkommunikation aller Behörden und Organisationen mit Sicherheitsaufgaben über das bundeseinheitliche Netz abzuwickeln. Das Digitalfunknetz BOS soll dabei, unabhängig von kommerziellen Mobilfunknetzen, eine hoch verfügbare und abhörsichere Kommunikation für die Einsatzkräfte der Behörden und Organisationen mit Sicherheitsaufgaben gewährleisten. Eine seiner Stärken ist die nahezu bundesweite Funkabdeckung: 99 Prozent des Bundesgebietes sind funkversorgt. Gleichzeitig bestehen vor allem im ländlichen Raum noch immer Lücken in den kommerziellen Mobilfunknetzen.

Im manchen Einsatzlagen zeigen sich jedoch auch Schwächen des Digitalfunk BOS. Neben Einschränkungen des Funkempfangs bei einigen massiven Gebäuden und Bahnhöfen kommt es insbesondere im Rahmen von Großeinsätzen oder Krisensituationen wiederholt zu Funkausfällen. So konnten während eines Stromausfalls am 16. Mai 2018 im Lübecker Stadtgebiet Polizei, Feuerwehr und Rettungsdienste für 23 Minuten keinen Kontakt zu ihrer Leitstelle aufbauen. Die unmittelbare Kommunikation der Einsatzkräfte untereinander war eingeschränkt (vgl. www.shz.de/regionales/luebeck/digitalfunk-ausgefallen-war-es-menschliches-versagen-id20003392.html). Auch während des Anschlags am bzw. im Münchener Olympia-Einkaufszentrum im Jahr 2016 kam es zu einem Zusammenbruch des Digitalfunks der bayerischen Polizei (vgl. www.sueddeutsche.de/muenchen/digitalfunk-warum-die-polizei-in-der-amok-nacht-ins-leere-funkte-1.3213229).

Darüber hinaus ist das BOS-Digitalfunknetz technisch nicht in der Lage, mittlere bis größere Dateien wie Foto- oder Videoaufnahmen zu übermitteln. Als Ersatz wurde Medienberichten zufolge häufig der Messengerdienst WhatsApp mit privaten Handys von Beamten genutzt. Obwohl die Nutzung von WhatsApp innerhalb der Polizei untersagt ist, greifen auch gegenwärtig noch viele Polizeibeamten auf ihre privaten Handys zurück, um Aufnahmen von Tatorten o. Ä. weiterzuleiten (vgl. www.nordbayern.de/region/digitalfunk-zu-langsam-polizeibekommt-dienst-iphones-1.6411620). Besonders problematisch an der Nutzung von WhatsApp sind die regelmäßigen Meldungen über Sicherheitslücken. So hat die israelische Sicherheitsfirma CheckPoint aktuell festgestellt, dass es für Hacker möglich ist, den Nachrichtenaustausch zu manipulieren (vgl. www.welt.de/newsticker/news1/article180826266/Cyberkriminalitaet-Sicherheitsfirma-entdeckt-Einfallstor-fuer-Hacker-auf-Whatsapp.html). Um eine gesicherte Datenübertragung im Einsatzalltag zu gewährleisten, wird in vielen Bundesländern nun die Einführung interner Messengerdienste diskutiert. So hat die bayerische Polizei im Mai 2017 mit der Einführung des „Polizei-Messengers“ begonnen. Genutzt wird die App Teamwire, bei der Nachrichten verschlüsselt auf einer gesicherten Plattform übertragen werden und auf einem Server in Deutschland landen. In weiteren Bundesländern befinden sich polizeiinterne Messengerdienste in der Testphase wie beispielsweise der „Niedersachsen Messenger“ (kurz: „Nimes“) in Niedersachsen.

Vorbemerkung der Bundesregierung

Soweit die Fragen 1, 2, 9 und 15 das Bundesamt für Verfassungsschutz (BfV) betreffen, ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Antwort nicht – auch nicht in eingestufte Form – erfolgen kann.

Die Antworten sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der nachrichtendienstlichen Arbeitsweise und Methodik stehen. Gegenstand der Fragen sind solche Informationen, die in besonderem Maße das Staatswohl berühren. Eine Bekanntgabe von Einzelheiten der technischen Mittel sowie deren konkreter Anwendung im BfV würde zu weitgehenden Rückschlüssen auf technische Fähigkeiten und Aufklärungspotenzial des BfV schließen lassen. Der Erfolg zukünftiger Maßnahmen könnte gefährdet und damit die Erkenntnisgewinnung beeinträchtigt werden. Diese ist zur Aufgabenerfüllung der Sicherheitsbehörden jedoch unerlässlich. Die notwendige Abwägung zwischen dem Geheimhaltungsinteresse einerseits und dem grundsätzlich umfassenden parlamentarischen Fragerecht andererseits ergibt daher, dass auch eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimchutzstelle des Deutschen Bundestages angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung des BfV und den zuvor benannten Gründen nicht in Betracht kommt, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann. Die angefragten Inhalte erfordern eine derart detaillierte Darstellung der technischen Fähigkeiten des BfV, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann.

1. Ist der Umstieg auf den Digitalfunk bei Einheiten bzw. Dienststellen
 - a) der Bundespolizei,
 - b) des Bundeskriminalamtes,
 - c) der Bundesanstalt Technisches Hilfswerk,
 - d) der Bundeszollverwaltung sowie
 - e) des Bundesamtes für Verfassungsschutzmit Stand zum 1. August 2018 vollständig vollzogen?

Soweit sich die Frage auf das BfV bezieht, wird auf die Vorbemerkung der Bundesregierung verwiesen.

Mit Stand zum 1. August 2018 ist der Umstieg auf den Digitalfunk beim Bundeskriminalamt und bei der Bundeszollverwaltung für alle dort vorgesehenen Fachbereiche bereits vollständig vollzogen.

Bei der Bundespolizei konnten die Ausstattung mit Handfunk- und Fahrzeugfunkgeräten abgeschlossen und die Digitalfunk-Kommunikation der Leitstellen bereits sichergestellt werden. Die Ausstattung mit ergänzender „Vermittlungstechnik Leitstellen“ (VTLST) soll bis Ende 2018 beendet sein.

Bei der Bundesanstalt Technisches Hilfswerk (THW) befindet sich derzeit in der vierten und letzten Phase – die Einrüstung der Dienststellen mittels fest eingebauter Sprechstellen. Die ersten drei Migrationsphasen Handfunkgeräte, Fahrzeugeinbauten und portabel einsetzbare Koffergeräte sind aber abgeschlossen. Zudem befindet sich in der Taktisch-Technischen Betriebsstelle der THW-Leitung bereits eine feste Sprechstelle im Pilotbetrieb.

2. Wenn ein vollständiger Umzug noch nicht vollzogen sein sollte, welche Einheiten bzw. Dienststellen sind noch nicht auf den Digitalfunk umgerüstet (bitte nach Behörde und Dienststelle aufschlüsseln)?

Soweit sich die Frage auf das BfV bezieht, wird auf die Vorbemerkung der Bundesregierung verwiesen.

Die Bundespolizei und das THW sind noch nicht vollständig auf den Digitalfunk umgerüstet. Zu den noch offenen Maßnahmen für einen vollständigen Umstieg wird auf die Antwort zu Frage 1 verwiesen.

3. Ist nach Kenntnis der Bundesregierung der Umstieg auf den Digitalfunk in den Bundesländern mit Stand zum 1. August 2018 vollumfänglich vollzogen?
Wenn nein, in welchen Bundesländern ist dies nicht der Fall, und welche dortigen Behörden bzw. Organisationen kommunizieren nach Kenntnis der Bundesregierung nicht mittels Digitalfunk?

Bund und Länder verzichten seit der Etablierung des Digitalfunks BOS sukzessive auf die Nutzung analoger Sprechfunktechnik und bauen diese schrittweise zurück. Der Rückbau in den Ländern erfolgt unterschiedlich und nach eigener Maßgabe.

4. Wie wird die gemeinsame Einsatzkommunikation in Situationen gelöst, in denen Einheiten von BOS beteiligt sind, die noch über Analogfunk kommunizieren?

Die gemeinsame Kommunikation wird bei der Bundespolizei und dem THW durch das Mitführen beider Gerätearten (Analog- und Digitalfunk) gewährleistet.

Zusätzlich wird beim THW ein Pool an Digitalfunkgeräten vorgehalten, um anderen Sicherheitsbehörden für den Zeitraum der Zusammenarbeit Geräte zur Verfügung stellen zu können.

5. Welche Erkenntnisse liegen der Bundesregierung zu Teil- und Totalausfällen des Digitalfunks in den Jahren 2016 bis 2018 vor (bitte nach Jahren und Vorkommnissen aufschlüsseln)?

Ein Totalausfall des Digitalfunks BOS gab es nicht. Beim BOS-Digitalfunknetz handelt es sich um das weltweit größte und – mit einer Verfügbarkeit von 99,97 Prozent – zugleich zuverlässigstes Digitalfunknetz seiner Art.

Folgende Teilausfälle sind im angefragten Zeitraum aufgetreten:

- März 2017, Bayern: Aufgrund eines Stromausfalls waren 69 Basisstationen für vier Minuten beeinträchtigt.
- Mai 2018, Schleswig-Holstein: Aufgrund eines Stromausfalls kam es zu Kapazitätseinschränkungen in einem Netzabschnitt für 23 Minuten.
- Mai 2018, Niedersachsen: Aufgrund eines Brandes innerhalb einer Vermittlungsstelle kam es zu Ausfällen von Leitstellenanbindungen; für einen Zeitraum 3 Stunden und 11 Minuten war kein Versand von Kurznachrichten möglich.

6. Welche Maßnahmen ergreift die Bundesregierung, um Teil- und Totalausfälle des Digitalfunks zu verhindern?

Alle für die Funktion des BOS-Digitalfunknetzes notwendigen Komponenten sind redundant ausgelegt. Grundsätzlich gewährleistet beim Ausfall des Versorgungsnetzes die Notstromversorgung einen Betrieb des gesamten Digitalfunks BOS für mindestens zwei Stunden. Darüber hinaus haben Bund und Länder im Rahmen der sogenannten „Netzhärtung“ beschlossen, die Notstromversorgung nach den Empfehlungen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) für das BOS-Digitalfunknetz auszubauen. Im Falle eines langandauernden Stromausfalls wird die Funkversorgung mit der GAN-Kategorie 0 (Funkversorgung mit Fahrzeugfunk) flächendeckend für mindestens 72 Stunden gewährleistet. Die Empfehlungen des BBK wurden für den Bereich des Kernnetzes bereits umgesetzt.

7. Welche Konsequenzen zieht die Bundesregierung aus dem Ausfall des Digitalfunks am 16. Mai 2018 in Lübeck aufgrund des Betriebsausfalls der Vermittlungsstellen?

Der kurzzeitige Ausfall des Digitalfunks BOS am 16. Mai 2018 an der Vermittlungsstelle Lübeck ist auf ein bis zu diesem Zeitpunkt nicht vorhersehbares, seltenes Fehlerbild zurückzuführen. Das für die Fehlfunktion (Nichtanlauf der Netzersatzanlagen) verantwortliche elektronische Bauteil wird in allen Vermittlungsstellen, in denen es baugleich im Einsatz ist, zeitnah ersetzt.

Grundsätzlich unterliegen alle wesentlichen technischen Komponenten einer regelmäßigen Überprüfung mit besonderem Blick auf die vom Hersteller angegebene Lebensdauer. Bereits vor Ablauf dieser Frist werden betroffene Komponenten genauer untersucht und ggf. vorab getauscht, um ein mögliches Ausfallrisiko zu minimieren.

8. Welche Maßnahmen hat die Bundesregierung seit der Einführung des Digitalfunks im Jahr 2016 ergriffen, um die Objektfunkversorgung in öffentlichen Gebäuden zu verbessern?

Bereits seit dem Jahr 2011 ist das sog. Anzeige- und Genehmigungsverfahren für Objektfunkanlagen für den Digitalfunk BOS etabliert. Dieses begleitet den gesamten Prozess der Anmeldung, Planung, Errichtung und Inbetriebnahme von Objektfunkanlagen, an deren Abschluss die rückwirkungsfreie Einbindung in das BOS-Digitalfunknetz steht. Über dieses Verfahren sind ca. 2 450 Anlagen realisiert worden. In Veranstaltungsreihen wird dieses Verfahren regelmäßig den Bedarfsträgern bei Bund, Ländern, Kommunen und Unternehmen präsentiert.

Ergänzend dazu wurde im Jahr 2016 ein Leitfaden zur Planung, Umsetzung und Inbetriebnahme von Objektversorgungsanlagen veröffentlicht. Der gegenwärtige Fokus liegt auf der Konzeptionierung von Lösungen zur Versorgung der Bahnhöfe und Tunnel der Deutschen Bahn AG und von Ballungsräumen mit Hilfe eines sog. „Metropoliskonzepts“.

Die meisten Gebäude werden bereits durch die Funkversorgung des Freifeldes mit abgedeckt, es gibt jedoch auch Bauwerke, deren Beschaffenheit eine zusätzliche Funkversorgung notwendig macht. So zum Beispiel Tunnelsysteme oder Gebäude mit abschirmendem Stahlbeton oder metallbedampften Fenstern. Um auch hier die Kommunikation zwischen den Einsatzkräften oder zwischen den Einsatzkräften und der Leitstelle zu gewährleisten, müssen diese Gebäude mit einer Objektfunkanlage ausgestattet werden.

Bei Neubauten der öffentlichen Hand und privater Betreiber wird die Versorgung des Gebäudeinneren mit Digitalfunk BOS im Rahmen des Baugenehmigungsverfahrens regelmäßig berücksichtigt und im Rahmen eines abgestimmten Vorgehens zwischen der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) und den Ländern an das Digitalfunknetz BOS angebunden. Für alle bestehenden Gebäude gilt gleichermaßen der baurechtliche Bestandsschutz. Änderungen baurechtlicher Regelungen liegen in der Gesetzgebungskompetenz der Länder.

Über die Schaffung einer (länder-) gesetzlichen Regelung hinaus unterstützen Bund, Länder und die BDBOS einen Diskussionsprozess, um die Eigentümer bzw. Betreiber für eine freiwillige Um- bzw. Ausrüstung ihrer Gebäude zu sensibilisieren. Hierdurch wird insbesondere im Bereich der Versammlungsstätten und des öffentlichen Personennahverkehr (ÖPNV) durch o. g. Maßnahmen eine stetig steigende Zahl von freiwilligen Um- bzw. Ausrüstungsmaßnahmen erreicht.

Die Forderungen nach Objektfunkanlagen zur Einsatzunterstützung der Feuerwehr im Brandschutz und im Rettungsdienst ist grundsätzlich Ländersache und demnach im Bauordnungsrecht (BauO) bzw. im Brand- und Katastrophenschutzrecht (hier beispielhaft am Land Nordrhein-Westfalen, § 29 Absatz 2 S. 4 des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz [BHKG]) verortet und wird durch die kommunalen Feuerwehren beim Objektbetreiber eingefordert.

Nach Kenntnis der Bundesregierung haben die Länder Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und das Saarland die rechtlichen Grundlagen für die Einrichtungen von Objektfunkanlagen in Bestandsobjekten bereits angepasst.

9. Welche alternativen Kommunikationswege sind für die Beamtinnen und Beamten der in Frage 1 genannten Sicherheitsbehörden des Bundes für den Fall einer Störung des Digitalfunks während eines laufenden Einsatzes vorgesehen?

Soweit sich die Frage auf das BfV bezieht, wird auf die Vorbemerkung der Bundesregierung verwiesen.

Der Digitalfunk gilt mit mehr als 99 Prozent tatsächlicher Verfügbarkeit als robust. Unabhängig davon bietet das Digitalfunksystem selbst verschiedene Betriebsmodi, mit dem auf unterschiedliche Szenarien – auch im Falle von Störungen – reagiert werden kann (bspw. Die Nutzung von „Notfall-Vermittlungsstellen“, die Nutzung des Fallback-Modus einer Basisstation oder die Kommunikation im Direktmodus zwischen Endgeräten(DMO)). Darüber hinaus wird auf dienstliche Mobiltelefone oder den Analogfunk ausgewichen.

Des Weiteren hält das THW feldmäßig einsetzbare draht- und DECT-gebundene Kommunikationssysteme für Einsatz- bzw. Schadensgebiete vor. Diese Systeme können zusätzlich durch vorgehaltene Technik an öffentliche Telefonnetze angeschlossen werden.

Die Kommunikation in Bestandsliegenschaften kann bei einem Ausfall über die NdB-Sprachanschlüsse erfolgen.

10. Bestehen seitens der Bundesregierung Pläne, die aktuell durch das BOS-Digitalfunknetz realisierte schmalbandige Datenkommunikation der BOS zu einer breitbandigen Datenkommunikation auszubauen (bitte erläutern)?

Die Weiterentwicklung des Digitalfunks BOS ist zwingend erforderlich, um die einsatzkritische Kommunikation der BOS und der Bundeswehr in Deutschland über das Jahr 2020 hinaus sicherzustellen.

Zur erforderlichen Sicherstellung der Hochverfügbarkeit wird in einem ersten Schritt das bestehende BOS-Digitalfunknetz bis Mitte 2021 auf den IP-Standard angehoben. Dies bildet die Voraussetzung für die anschließende Realisierung der Anforderungen eines Breitbandnetzes.

11. Welche Regelungen gelten für die Nutzung von privaten Mobiltelefonen der Beamtinnen und Beamten der in Frage 1 genannten Sicherheitsbehörden des Bundes für dienstliche Kommunikation?

In den Behörden ist ausschließlich die Nutzung dienstlicher Geräte erlaubt. Die dienstliche Kommunikation über private Geräte (u. a. Mobiltelefone, PDA, Notebooks, Tablets und Smartphones) ist grundsätzlich nicht gestattet.

12. Welche Schlussfolgerungen zieht die Bundesregierung aus Berichten über Sicherheitslücken bei Messengerdiensten wie WhatsApp für die dienstliche Kommunikation der in Frage 1 genannten Sicherheitsbehörden des Bundes?

Die öffentlich zugänglichen Messengerdienste wie z. B. Whatsapp sind aus Gründen der IT-Sicherheit und des Informationsschutzes für die dienstliche Kommunikation nicht geeignet und aus diesen Gründen nicht erlaubt.

13. Sind der Bundesregierung Fälle bekannt, in denen versucht worden ist, Einfluss auf die Einsatzkommunikation der in Frage 1 genannten Sicherheitsbehörden des Bundes über den Messengerdienst WhatsApp zu nehmen?

Wenn ja, in welcher Art und Weise?

Derartige Fälle sind nicht bekannt.

14. Ist aus Sicht der Bundesregierung ein ergänzendes Mittel in der Einsatzkommunikation von BOS erforderlich?

Wenn ja, welche alternativen Kommunikationsmittel kommen aus Sicht der Bundesregierung in Betracht?

Ein sicherer, plattformunabhängiger und behördenübergreifender Messengerdienst für die (genannten Sicherheits-)Behörden ist sinnvoll.

Eine Produktspezifikation muss im Rahmen einer Ausschreibung erstellt werden.

15. Wird bei den in Frage 1 genannten Sicherheitsbehörden des Bundes ein behördeninterner Messengerdienst verwendet bzw. erprobt?

Wenn ja, um welchen handelt es sich?

Wenn nein, plant die Bundesregierung entsprechende Erprobungen, Pilotprojekte o. Ä.?

Soweit sich die Frage auf das BFV bezieht, wird auf die Vorbemerkung der Bundesregierung verwiesen.

Bei der Bundespolizei wird derzeit ein IT-Verfahren mit dem internen Namen „MOKA (Mobile Ortungs- und Kommunikationsanwendung)“ erprobt, welches auf – gem. Vorgaben der IT-Sicherheit und des UA IuK – konfigurierten und gemanagten mobilen Endgeräten (Smartphones) im Rechenzentrum der Bundespolizei betrieben wird. Die Kommunikation erfolgt über das Internet unter Nutzung eines geeigneten Verschlüsselungsverfahrens der Datenübertragung (VPN).

Zusätzlich ist auch noch die Kommunikation der MOKA-App gem. einschlägigen Richtlinien des BSI transportverschlüsselt. Technisch besteht das System aus verschiedenen Open-Source-Softwarekomponenten auf Basis des offenen Protokollstandards XMPP (Extensible Messaging and Presence Protocol), die durch die Bundespolizei integriert und betrieben werden.

Gemäß Beschluss des AK II in der 255. Sitzung vom 11./12. April 2018 in Erfurt wurde das BKA gebeten, das Produkt SE-Netz des Fraunhofer-Instituts IVI in Dresden als bundeseinheitliche Lösung für ein Einsatz-Kommunikations- und Unterstützungssystem (EKUS) bereitzustellen und zu betreiben. Dieses Produkt, das sich an die polizeilichen Spezialeinheiten des Bundes und der Länder richtet, verfügt unter anderem über eine marktgängiger Produkte entsprechende Messenger-Funktionalität. Das Produkt wird derzeit auch in der Zollverwaltung erprobt.

Darüber hinaus prüft das Bundeskriminalamt (BKA) gegenwärtig die Verwendung des Produkts SecurePIM der Firma Virtual Solution, das perspektivisch ebenfalls über eine Messenger-Funktionalität verfügen wird. Eine Entscheidung über die Verwendung dieses Produkts steht noch aus.

16. Wie bewertet die Bundesregierung die Nutzung von behördeninternen Messengerdiensten mit Blick auf datenschutzrechtliche Bestimmungen, insbesondere hinsichtlich des Umgangs mit personenbezogenen Daten bzw. datenschutzrechtlichen Bestimmungen?

Für einen Messengerdienst gelten keine anderen datenschutzrechtlichen Bestimmungen als für die übrigen IT-Verfahren der Behörden.

17. Welche Schlussfolgerungen zieht die Bundesregierung aus dem Pilotprojekt der bayerischen Polizei, die Smartphones für den Dienstgebrauch angeschafft und mit einem polizeiinternen Messengerdienst ausgestattet hat?

Das Pilotprojekt ist nicht ausreichend bekannt, um dies bewerten zu können.

Die Bundesregierung unterscheidet zwischen einsatzkritischer und einsatzunkritischer Kommunikation. Jegliche einsatzkritische Kommunikation der BOS und Bundeswehr soll in einem einheitlichen, sicheren und gehärteten Netz gewährleistet werden.

Dies bietet nur der Digitalfunk BOS. Zur Evaluierung der Deckung des Bedarfs an geschützter breitbandiger Kommunikation ist daher – vorbehaltlich noch ausstehender Beschlüsse der Innenministerkonferenz sowie nachfolgend des Verwaltungsrats der BDBOS – die Pilotierung eines hochverfügbaren und abhörsicheren Breitbandnetzes geplant, welches das existierende BOS-Digitalfunknetz perspektivisch ergänzen kann.