

Kleine Anfrage

der Abgeordneten Benjamin Strasser, Stephan Thomae, Renata Alt, Nicole Bauer, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Otto Fricke, Katrin Helling-Plahr, Torsten Herbst, Katja Hessel, Manuel Höferlin, Reinhard Houben, Olaf in der Beek, Ulla Ihnen, Gyde Jensen, Dr. Christian Jung, Thomas L. Kemmerich, Pascal Kober, Konstantin Kuhle, Oliver Luksic, Alexander Müller, Roman Müller-Böhm, Hagen Reinhold, Dr. Stefan Ruppert, Thomas Sattelberger, Dr. Wieland Schinnenburg, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Katja Suding, Linda Teuteberg, Gerald Ullrich, Johannes Vogel (Olpe) und der Fraktion der FDP

Digitalfunk und Einsatzkommunikation

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-polizei-bekommt-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.

Wir fragen die Bundesregierung:

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 Verfassungsschutz mit Stand zum 1. August 2018 vollständig vollzogen?
2. Wenn ein vollständiger Umzug noch nicht vollzogen sein sollte, welche Einheiten bzw. Dienststellen sind noch nicht auf den Digitalfunk umgerüstet (bitte aufschlüsseln nach Behörde und Dienststelle)?
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?
4. Wie wird die gemeinsame Einsatzkommunikation in Situationen gelöst, in denen Einheiten von BOS beteiligt sind, die noch über Analogfunk kommunizieren?
5. Welche Erkenntnisse liegen der Bundesregierung zu Teil- und Totalausfällen des Digitalfunks in den Jahren 2016-2018 vor (bitte aufgeschlüsselt nach Jahren und Vorkommnissen)?
6. Welche Maßnahmen ergreift die Bundesregierung, um Teil- und Totalausfälle des Digitalfunks zu verhindern?
7. Welche Konsequenzen zieht die Bundesregierung aus dem Ausfall des Digitalfunks am 16. Mai 2018 in Lübeck aufgrund des Betriebsausfalls der Vermittlungsstellen?

8. Welche Maßnahmen hat die Bundesregierung seit der Einführung des Digitalfunk im Jahr 2016 ergriffen, um die Objektfunkversorgung in öffentlichen Gebäuden zu verbessern?
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?
10. Bestehen seitens der Bundesregierung Pläne, die aktuell durch das BOS-Digitalfunknetz realisierte schmalbandige Datenkommunikation der BOS zu einer breitbandigen Datenkommunikation auszubauen (bitte erläutern)?
11. Welche Regelungen gelten für die Nutzung von privaten Mobiltelefonen der Beamtinnen und Beamten der o. g. Sicherheitsbehörden des Bundes für dienstliche Kommunikation?
12. Welche Schlussfolgerungen zieht die Bundesregierung aus Berichten über Sicherheitslücken bei Messengerdiensten wie WhatsApp für die dienstliche Kommunikation der o. g. Sicherheitsbehörden des Bundes?
13. Sind der Bundesregierung Fälle bekannt, in denen versucht worden ist, Einfluss auf die Einsatzkommunikation der o. g. Sicherheitsbehörden des Bundes über den Messengerdienst Whatsapp zu nehmen?
Wenn ja, in welcher Art und Weise?
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?
15. Wird bei den o. g. 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.?
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?
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?

Berlin, den 22. August 2018

Christian Lindner und Fraktion

