Deutscher Bundestag **Drucksache 19/11396**

19. Wahlperiode 04.07.2019

Kleine Anfrage

der Abgeordneten Andrej Hunko, Heike Hänsel, Michel Brandt, Dr. Diether Dehm, Anke Domscheit-Berg, Dr. André Hahn, Ulla Jelpke, Niema Movassat, Thomas Nord, Petra Pau, Tobias Pflüger, Alexander Ulrich und der Fraktion DIE LINKE.

Europäische Initiativen zur Überwachung der 5G-Telefonie

Die fünfte Mobilfunkgeneration (5G) ermöglicht Telefonverbindungen mit etappenweiser Verschlüsselung. Deutsche Polizeien und Geheimdienste befassen sich deshalb seit längerer Zeit mit Möglichkeiten des Zugangs zu diesen sicheren Verbindungen (Bundestagsdrucksache 19/10535, Schriftliche Frage 18 des Abgeordneten Dr. Diether Dehm). Die Bundesregierung bezeichnet dies als „Herausforderungen“ für ihre Sicherheitsbehörden. Dies betreffe die Gefahrenabwehr und die Strafverfolgung (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765).

Die technische Standardisierung von 5G ist noch nicht abgeschlossen und soll im Dezember 2019 finalisiert werden (Ratsdokument 8983/19). Daher ist es noch möglich, die Implementierung von Abhörschnittstellen bei der Einführung von 5G zu berücksichtigen. Die Bundesregierung beteiligt sich mit dem Bundesamt für Verfassungsschutz (BfV), der Bundesnetzagentur (BNetzA) und dem Zollkriminalamt (ZKA) an dem Europäischen Institut für Telekommunikationsnormen (ETSI) bzw. dort eingerichteten Arbeitsgruppen zu Abhörmöglichkeiten (Bundestagsdrucksache 17/11239, Frage 10). Das Bundeskriminalamt (BKA) nimmt nicht daran teil, stimmt sich aber mit dem ZKA inhaltlich zu gemeinsamen Positionen ab. Im März 2012 hatte das ETSI 759 Mitglieder aus 62 Ländern, im Jahr 2011 betrug das Budget 22 472 000 Euro (www.etsi.org/membership).

Zusammen mit der BNetzA nimmt das BfV seit 2003 außerdem am 3rd Generation Partnership Project (3GPP) zu „Lawful Interception“ (SA3-LI) teil. Das 3GPP, dem sich auch das ETSI angeschlossen hat, ist ein weltweiter Zusammenschluss von sieben Standardisierungsgremien. Zu ihnen gehören neben Behörden auch Netzwerkausrüster und Netzbetreiber sowie „Hersteller von Sicherheitstechnik und Überwachungslösungen“ (Bundestagsdrucksache 17/11239, Frage 10). Voraussetzung für die Mitarbeit in 3GPP ist die Mitgliedschaft in einem der dort zusammengeschlossenen Standardisierungsgremien (für die Bundesbehörden das ETSI). Laut einem Medienbericht hat die 3GPP-Arbeitsgruppe SA3-LI bereits dafür gesorgt, dass die Interessen der Behörden „gewürdigt werden“ („Verschlüsselung in 5G: ‚Das Rennen ist verloren‘“, www.heise.de vom 6. Juni 2019). Bezüglich der Abhörschnittstellen für Behörden entsprechen die neuen 5G-Standards früheren Mobilfunkstandards.

Für mehr Sicherheit soll in 5G die Verschlüsselung der bislang unverschlüsselt übertragenen Teilnehmerkennungen (IMSI) sorgen. Daher sind sogenannte IMSI-Catcher, mit denen die Nummern von in der Nähe befindlichen Telefonen festgestellt oder mit einer fingierten Netzstation abgehört werden können, nutzlos. Das bestätigt auch die Bundesregierung (siehe oben) und prüft, mit welchen „technischen und rechtlichen Anpassungen“ diese „derzeitige Konfiguration“ des 5G-Standards im Rahmen des Standardisierungsprozesses im ETSI geändert werden könnte. Möglich wäre, dass die IMSI- oder IMEI-Daten zukünftig mit richterlichem Beschluss bei den Netzanbietern abgefragt werden können („Verschlüsselung in 5G: ‚Das Rennen ist verloren‘“, www.heise.de vom 6. Juni 2019).

Auch die EU-Justiz- und -Innenminister haben sich auf ihrer Tagung am 6. und 7. Juni 2019 mit Auswirkungen von 5G auf dem Gebiet der inneren Sicherheit befasst („Überwachungs-Overkill im EU-Ministerrat ab Donnerstag“, https://fm4. orf.at vom 2. Juni 2019). Diskussionsgrundlage war das erwähnte Papier des EU-Koordinators für Terrorismusbekämpfung. Gilles de Kerchove wurde dabei vom BKA unterstützt, wofür sich dieser ausdrücklich bedankt hat. Das BKA hatte bei einem Termin „Informationen zu möglichen Auswirkungen von 5G auf die Aufgabenwahrnehmung der Sicherheitsbehörden“ zur Verfügung gestellt (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765).

Wir fragen die Bundesregierung:

1. Worin bestehen aus Sicht der Bundesregierung die „Herausforderungen“ für die Sicherheitsbehörden hinsichtlich der fünften Mobilfunkgeneration (5G), die sie in den Bereichen Gefahrenabwehr und Strafverfolgung feststellt und die den Zugang zu relevanten Informationen für die Behörden betreffen (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765)?

2. Besteht aus Sicht der Bundesregierung die ernsthafte Gefahr, dass die vorhandenen Ermittlungsmaßnahmen im Bereich der Telekommunikation nach Einführung der 5G-Technologie faktisch nicht mehr oder nicht mehr im gleichen Umfang zur Verfügung stehen und dadurch Ermittlungslücken entstehen (vgl. Jumiko-Frühjahrskonferenz 2019, Beschluss zur „Sicherung der Möglichkeit der Telekommunikationsüberwachung bei Einführung der fünften Mobilfunkgeneration)?

   Falls ja, worin liegt diese Gefahr konkret?

   Falls nein, welche Ermittlungsmaßnahmen gemäß §§ 100a ff. der Strafprozessordnung werden aus Sicht der Bundesregierung mit der Einführung des 5G-Standards nach derzeitigem Stand nicht beeinträchtigt?

   a) Enthalten die vom ETSI und dem 3GPP entwickelten bzw. diskutierten Standards zu 5G nach Kenntnis der Bundesregierung nach derzeitigem Stand eine Option, eine Pflicht oder eine Empfehlung für Ende-zu-Ende-Verschlüsselung?

   b) Welche Ermittlungslücken sieht die Bundesregierung hinsichtlich des Roamings mittels eines Endgeräts, das in Deutschland genutzt wird, aber bei einem ausländischen Netzbetreiber angemeldet ist?

   c) Sieht die Bundesregierung Ermittlungslücken hinsichtlich der in 5G möglichen Aufteilung in eine Vielzahl virtueller Netze („Network Slicing“)?

      Falls ja, wodurch kommen diese zustande?

d) Inwiefern haben sich bereits unter 4G entsprechende Ermittlungslücken gezeigt, das nach Kenntnis der Fragestellerinnen und Fragesteller mit einem „Dedicated Core Network“ (DCN) ebenfalls in verschiedene Netze unterteilt werden kann (bitte erläutern)?

e) Handelt es sich bei dem in 5G genutzten „Multi-Access Edge Computing“ (MEC) am Endgerät aus Sicht der Bundesregierung um die Verarbeitung von Kommunikationsdaten oder um eine Datenverarbeitung auf dem Endgerät?

f) Welche Möglichkeiten kennt und nutzt die Bundesregierung zur Ausleitung dieser „Access Edge“-Daten?

3. Inwiefern gelten die beschriebenen Gefahren oder Ermittlungslücken nach Kenntnis der Bundesregierung auch für Endgeräte, die neben 5G zunächst das 4G-Kernnetz verwenden oder über Schnittstellen für 4G, 3G bzw. 2G verfügen?

4. Welche dieser beschriebenen Gefahren existieren nach Auffassung der Bundesregierung in welchem Modell des Parallelbetriebs von EPC (4G Core) und 5G?

5. Steigt nach Ansicht der Bundesregierung durch Verfahren in 5G wie beispielsweise MEC die Wahrscheinlichkeit, dass überwachte Telekommunikationskundinnen und -kunden von laufenden Überwachungsmaßnahmen erfahren?

6. Über welche Fähigkeiten, Ausrüstung und Kompetenzen verfügen Bundesbehörden bzw. nach Kenntnis der Bundesregierung auch Behörden der Länder zur Telekommunikationsüberwachung von Netzen auf Basis des Codemultiplexverfahrens (CDMA-/CDMA2000)?

7. Inwiefern bzw. mit welchen Einschränkungen können deutsche Sicherheitsbehörden die Abhörmöglichkeiten oder Schnittstellen zur Ausleitung von Telekommunikationsdaten, die hinsichtlich der Standards 4G, 3G bzw. 2G genutzt werden, für 5G weiter verwenden?

8. Inwiefern trifft es aus Sicht der Bundesregierung zu, dass IMSI-Catcher unter 5G sämtlich nicht mehr nutzbar sind?

a) Welche konkreten Informationen (etwa Inhalte, Zeit und Dauer des Gesprächs, Angerufene, IMSI- und IMEI-Nummer) sind mit den von Bundesbehörden genutzten IMSI-Catchern nicht mehr zu überwachen?

b) Auf welche Weise können deutsche Behörden auch mit 5G an die „International Mobile Subscriber Identity“-Nummern (IMSI) der Telefone gelangen?

c) Welche IMSI-Catcher kennt die Bundesregierung, die auch eine Überwachung von 5G-Telefonie ermöglichen?

d) Welche Förderung oder Auftragsvergabe im Bereich der Forschung und Entwicklung von IMSI-Catchern gab es durch den Bund seit 2014?

9. Welche deutschen Behörden nehmen an Sitzungen des European Telecommunications Standards Institute (ETSI) und der Arbeitsgruppe „Strafverfolgung“ (SA3-LI) im 3rd Generation Partnership Project (3GPP) teil, bzw. welche Änderungen haben sich seit Beantwortung der Bundestagsdrucksachen 18/7466 und 17/11239 ergeben?

   a) Welche Arbeitsgruppentreffen (Plenary) und Rapporteurs-Sitzungen der Gruppe „Strafverfolgung“ (TC LI) des ETSI sowie der Arbeitsgruppe „Strafverfolgung“ des 3GPP haben nach Kenntnis der Bundesregierung im Jahr 2018 und 2019 stattgefunden, und wo wurden diese jeweils abgehalten?

   b) Welche Mitglieder der TC LI oder der SA3-LI haben nach Kenntnis der Bundesregierung die Arbeitsgruppentreffen (Plenary) und Rapporteurs-Sitzungen vorbereitet, und wer war für die Tagesordnung sowie die Organisation zuständig?

   c) Wer nahm an diesen Treffen teil (bitte wie auf Bundestagsdrucksache 17/11239 beantworten)?

10. Welche konkreten Punkte standen nach Kenntnis der Bundesregierung jeweils auf der Tagesordnung von Treffen der TC LI oder der SA3-LI in den Jahren 2018 und 2019, und welche Dokumente wurden hierfür im Vorfeld oder am Tag der Treffen verteilt?

    Was war der Inhalt der Tagesordnung?

    a) Welche ILETS-Sitzungen haben hierzu im Vorfeld stattgefunden, und welche Bundesbehörden beteiligten sich daran?

    b) Welche technischen Lösungen und Lösungsansätze unter Berücksichtigung verschiedener nationaler Gesetzgebungen wurden hinsichtlich von Schnittstellen zum Abhören von 5G bzw. der Nutzung von IMSI-Catchern bzw. vergleichbarer Verfahren in den ILETS-Gruppen, der TC LI und der SA3-LI vorgestellt und/oder diskutiert (bitte erläutern)?

11. Inwiefern haben sich das ZKA oder das BfV hinsichtlich der Standardisierung von 5G in den ILETS-Gruppen, der TC LI und der SA3-LI mit dem BKA abgestimmt?

    a) Welche eigenen Diskussionspapiere oder Vorschläge zu Herausforderungen von 5G oder Lösungsmöglichkeiten haben deutsche Behörden in den ILETS-Gruppen, der TC LI und der SA3-LI verteilt?

    b) Welche Berichte (Technical Reports) zu Möglichkeiten der Überwachung von 5G wurden nach Kenntnis der Bundesregierung in ILETS-Gruppen, der TC LI und der SA3-LI erstellt?

12. Wann sollen die nächsten Versionen des Standards zu 5G nach Kenntnis der Bundesregierung vom ETSI bzw. dem 3GPP veröffentlicht werden (Release #16), und welche technischen Spezifikationen zu Überwachungsmöglichkeiten stehen jetzt schon fest bzw. welche sollen nicht mehr verhandelt oder geändert werden (vgl. Ratsdokument 8983/19)?

    Werden bis zur Veröffentlichung nur noch Fehlerkorrekturen vorgenommen?

13. Was ist der Bundesregierung über eine 5G-Arbeitsgruppe bei der EU-Polizeiagentur Europol bekannt (Ratsdokument 8983/19), wer nimmt daran teil, und wie oft trifft sich diese?

    a) Was ist der Bundesregierung darüber bekannt, inwiefern Europol bereits an Treffen der ILETS-Gruppen, der TC LI und der SA3-LI teilnahm oder diese indirekt (etwa über das BKA oder das BfV) inhaltlich mitbestimmt hat?

    b) Welche Haltung vertritt die Bundesregierung zum Vorschlag des EU-Koordinators für Terrorismusbekämpfung, dass Europol Mitglied des ETSI werden könnte, um darüber Einfluss auf die dort oder bei 3GPP angesiedelten Arbeitsgruppen „Strafverfolgung“ zu nehmen?

14. Welche konkreten Mitarbeiterinnen und Mitarbeiter des BKA oder anderer Behörden beraten hierzu mit Europol, und inwiefern handelt es sich dabei um „heads of telecommunications interception units“ (Ratsdokument 8983/19)?

    a) Welche „Informationen zu möglichen Auswirkungen von 5G auf die Aufgabenwahrnehmung der Sicherheitsbehörden“ hat das BKA dem EU-Koordinator für Terrorismusbekämpfung zur Verfügung gestellt?

    b) Welche wesentlichen Bestandteile dieser BKA-Informationen sind aus Sicht der Bundesregierung in das Diskussionspapier des EU-Koordinators für Terrorismusbekämpfung eingeflossen (Ratsdokument 8983/19)?

    c) Haben das BKA oder Europol Gespräche hinsichtlich der Standardisierung von 5G oder ETS nach Kenntnis der Bundesregierung mit den Netzbetreibern Ericsson und Nokia geführt?

    Wenn ja, wie viele, und was waren die konkreten Gesprächsgegenstände?

15. Welche Vorgaben plant die Bundesregierung bei der Vergabe von 5G-Lizenzen für die Netzbetreiber hinsichtlich der Implementierung von Schnittstellen zum Abhören oder Ausleiten von Kommunikation, der Einrichtung zentraler Kommunikationsknoten, der Fragmentierung des Netzes oder dem Grad der Verschlüsselung?

    a) Sollen die Firmen eine komplette und entschlüsselte Kopie der Kommunikation bereithalten und/oder Schnittstellen hierfür einrichten?

    b) Sollen die Firmen ihre Netzwerke so organisieren, dass jederzeit Geodaten zur Lokalisierung der Telefone protokolliert werden?

    c) Sollen die Firmen dafür Sorge tragen, dass weiterhin IMSI-Catcher eingesetzt werden können?

16. Auf welche Weise könnte die Europäische Union aus Sicht der Bundesregierung die Bedürfnisse der Sicherheitsbehörden nach Abhörmöglichkeiten bei der Standardisierung von 5G unterstützen (vgl. Ratsdokument 8983/19)?

    a) Welche Ratsarbeitsgruppen sind nach Kenntnis der Bundesregierung derzeit mit der Überwachung von 5G befasst, und welche ist hierzu federführend, und wer sitzt dort von Seiten der Bundesregierung?

    b) Welche Unterstützung leisten nach Kenntnis der Bundesregierung die Agentur der Europäischen Union für Cybersicherheit (ENISA) oder das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) hinsichtlich der Bedürfnisse der Sicherheitsbehörden nach Abhörmöglichkeiten bei der Standardisierung von 5G und ETS?

    c) Sollte die Überwachung von 5G-Telefonie aus Sicht der Bundesregierung in die geplanten EU-Verordnungen zur Sicherung und Herausgabe elektronischer Beweismittel aufgenommen werden oder ist diese davon aus ihrer Sicht bereits umfasst?

17. Welche Position vertritt die Bundesregierung im ETSI hinsichtlich der Bereitstellung einer „Cloud Lawful Interception Function“ für Polizeien und Geheimdienste (Bundestagsdrucksache 17/11239, Frage 16)?

    a) Inwieweit befassen sich die ILETS-Gruppen, die TC LI und die SA3-LI nach Kenntnis der Bundesregierung auch mit dem Zugriff von Polizeien und Geheimdiensten auf Cloud-Daten, und welche Standardisierungen wurden hierzu verabredet oder diskutiert?

    b) Welche der hierzu in der Vergangenheit diskutierten Standards zur Überwachung von Clouddaten, die in einem Draft Technical Report veröffentlicht wurden, sind nach Kenntnis der Bundesregierung in Deutschland umgesetzt?

18. Welche Bedeutung misst die Bundesregierung der vom Massachusetts Institute of Technology vorgenommen Einstufung des vom ETSI entwickelten Protokolls Enterprise Transport Security (ETS) als Schwachstelle bei („Transport-Verschlüsselung: ETS aka eTLS ist laut MITRE-Schwachstellenliste ein Bug“, www.heise.de vom 12. Juni 2019), und wird sie sich deshalb für den Verschlüsselungsstandard TLS 1.3 einsetzen?

19. Mit welchen Behörden nimmt die Bundesregierung an der „Internet Engineering Task Force“ (IETF) teil, die sich mit der sicheren Verschlüsselung in zukünftigen Kommunikationsstandards befasst?

20. Wer nimmt an den auf Bundestagsdrucksache 19/10803, Antwort zu Frage 5 genannten Projekten des Forschungsinstituts Cyber Defence (CODE) an der Universität der Bundeswehr München im Handlungsfeld „Künstliche Intelligenz“ teil, und wann sollen die Ergebnisse vorliegen?

21. Welche Rahmenbedingungen existieren heute, um eine „aktive Cyber-Abwehr“ zu gestalten, und welche weiteren Rahmenbedingungen wären nötig, um diese auszubauen (http://gleft.de/2Ye, bitte ausführen, welche Haltung das Bundesministerium der Verteidigung bzw. dessen Generalleutnant Ludwig Leinhos hierzu vertritt)?

22. Welche Cybersicherheitsrisiken sind der Bundesregierung in 5G-Netzen bekannt, und wie werden diese von der Europäischen Kommission konkret adressiert (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

    a) Welche Risiken von 5G-Netzen hat die Bundesregierung auf nationaler Ebene identifiziert?

    b) Mit welchen EU-Institutionen trifft die Bundesregierung eine gemeinsame Risikoeinschätzung, und wie bringt sie sich hierzu auf EU-Ebene ein?

23. Welche Maßnahmen unternimmt nach Kenntnis der Bundesregierung die Kooperationsgruppe für Netz- und Informationssicherheit (NIS), um die Risiken für die „Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen“ – insbesondere 5G Netze – abzuschwächen (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

24. Welche „sensibelsten Elemente, bei denen Sicherheitsvorfälle [in 5G-Netzen] erhebliche negative Auswirkungen nach sich ziehen würden“, will die Bundesregierung der Europäischen Kommission bis 30. Juni 2019 mitteilen (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

Berlin, den 18. Juni 2019

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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.betrifft-gesetze.de
ISSN 0722-8333