Deutscher Bundestag **Drucksache 19/14046**

19. Wahlperiode 16.10.2019

Antrag

der Abgeordneten Manuel Höferlin, Frank Sitta, Jimmy Schulz, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Dr. Marco Buschmann, Carl-Julius Cronenberg, Britta Katharina Dassler, Bijan Djir-Sarai, Dr. Marcus Faber, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Carina Konrad, Konstantin Kuhle, Alexander Graf Lambsdorff, Michael Georg Link, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Hagen Reinhold, Christian Sauter, Matthias Seestern-Pauly, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Stephan Thomae, Johannes Vogel (Olpe), Nicole Westig und der Fraktion der FDP

Smart Germany – Cybersicherheit der 5G-Netze

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

5G stellt den Mobilfunk-Standard unserer Zukunft dar. Spitzenraten von bis zu 10 Gbit/s im Endausbau, deutlich geringere Latenzzeiten und höhere Verbindungsstabilitäten sind nur einige der Vorteile. Somit bietet die 5G-Technologie gerade bei Industrieanwendungen ein großes Potenzial zur Effizienzsteigerung, beispielsweise durch entkabelte Produktions- und Transportprozesse. Unterhalten Unternehmen auf dem Werksgelände eigene Mobilfunkstationen, lässt sich die Latenz durch den Wegfall von zusätzlichen Routern sogar auf rund 1 Millisekunde reduzieren und eröffnet so neue Möglichkeiten für fahrerlose Transportsysteme oder Virtual Reality Systeme in der Produktion. Ein weiteres Zukunftsfeld, das sich über 5G eröffnen lässt, ist der teilautonome und autonome Straßenverkehr. Die sehr kurze Signallaufzeit ermöglicht eine Datenübertragung nahezu in Echtzeit und bietet somit eine schier endlose Palette an Innovationsmöglichkeiten. Angefangen mit Stau- oder Unfallwarnungen in Echtzeit über automatisierte Erkennung von Fußgängern, Radfahrern oder anderen Verkehrsteilnehmern bis hin zu Systemen zur autonomen Kolonnenbildung oder Kreuzungsassistenz.

In all diesen Anwendungsfeldern ist auch ein höchstmöglicher Sicherheitsstandard Voraussetzung. Die 5G-Technologie bringt an sich schon ein höheres Schutzniveau mit als bisherige mobile Internetstandards. So ist die Kommunikation beispielsweise standardmäßig Ende-zu-Ende-verschlüsselt, Funkzellen müssen sich vor einer Verbindung gegenüber den Geräten authentifizieren, die IMSI

(International Mobile Subscriber Identity) wird nur verschlüsselt übertragen und eine direkte Verbindung zwischen zwei Geräten (Device-to-Device-Kommunikation) ist unter Umgehung der Funkmasten möglich. Darüber hinaus wird in Deutschland eine berechtigte Debatte über sichere und weniger sichere Anbieter von Netzwerkkomponenten in der 5G-Technologie geführt, da die Technik, die beim Ausbau von 5G zum Einsatz kommt, insbesondere in kritischen Infrastrukturbereichen höchste Sicherheitsstandards erfüllen muss.

Auch die Bundesregierung stellt in einem Bericht des Bundesministerium für Wirtschaft und Energie zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur die Relevanz der IT-Sicherheit in 5G-Netzen klar: "Angesichts der Bedeutung von 5G für die künftige Wettbewerbsfähigkeit des Standortes muss die Technik, die beim Ausbau von 5G zum Einsatz kommt, höchste Sicherheitsstandards erfüllen. Sicherheitsbedenken müssen so weit wie möglich ausgeschlossen werden. Das gilt für die eingesetzte Hard- und Software gleichermaßen." (Quelle: "Bericht der Bundesregierung zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur und ggf. erster Schlussfolgerungen daraus auf Grundlage der Empfehlung der Kommission vom 26.03.2019 Cybersicherheit der 5G-Netze", Ausschuss-Drucksache 19(23)053, S. 4) Ebenso erkennt die Europäische Kommission die strategische Relevanz der Gewährleistung der Cybersicherheit von 5G-Netzen für die Europäische Union und misst dieser eine entscheidende Bedeutung für die Gewährleistung der strategischen Autonomie der Europäischen Union bei. In ihrer Empfehlung vom 26.03.2019 zur "Cybersicherheit der 5G-Netze" (Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019) zeigt die Europäische Kommission zudem auf, dass sich Schwachstellen bzw. Cybersicherheitsvorfälle in den 5G-Netzen eines Mitgliedstaates aufgrund der Vernetzung auf die ganze Union auswirken können.

Doch gerade die Tatsache, dass dieses Sicherheitsniveau auch die Abhörsicherheit betrifft und verbessert, scheint die Bundesregierung zu stören. So prüft die Bundesregierung derzeit, "welche technischen und rechtlichen Anpassungen erforderlich sind, um zu gewährleisten, dass die Sicherheitsbehörden auch vor dem Hintergrund der Einführung des 5G-Standards ihren gesetzlichen Aufgaben nachkommen können" (Antwort der Bundesregierung auf die schriftliche Einzelfrage des Abgeordneten Dr. Diether Dehm (DIE LINKE.), Nr. 18 auf BT-Drs. 19/10535) und Bundesinnenminister Seehofer möchte noch in diesem Jahr Messenger gesetzlich zur Entschlüsselung zwingen (Quelle: https://www.spiegel.de/netzwelt/netzpolitik/horst-seehofer-will-messengerdienste-zum-entschluesseln-zwingen-a-1269121.html).
Auch in Hinblick auf den noch laufenden Standardisierungsprozess zu 5G unterstützt die Bundesregierung laut der Antwort auf die oben genannte schriftliche Einzelfrage das Engagement der Strafverfolgungsbehörden in den Standardisierungsgremien des ETSI (Europäisches Institut für Telekommunikationsnormen) und 3GPP (3rd Generation Partnership Project) und somit auch deren Ausarbeitungen bzgl. Abhörschnittstellen zur Ausleitung von Verkehr in den jeweiligen Spezifikationen (Quelle: https://www.heise.de/newsticker/meldung/Verschluesselung-in-5G-Das-Rennen-ist-verloren-4440605.html). Im Juni 2019 wurde sogar zusätzlich die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) durch das Bundesministerium des Innern, für Bau und Heimat in die Abhörarbeitsgruppen des ETSI und des 3GPP entsandt (Quelle: https://www.heise.de/tp/features/Huerden-bei-der-Ueberwachung-Wie-Behoerden-die-5G-Telefonie-verunsichern-4516624.html). All diese Entwicklungen deuten darauf hin, dass die Bundesregierung ihren Fokus im Standardisierungsprozess zu 5G mehr auf die Aufrechterhaltung oder gar Ausweitung der technischen Möglichkeiten der Strafverfolgungsbehörden bei der Überwachung

legt als die Chancen für einen gestärkten digitalen Schutz der Bürgerinnen und Bürger zu ergreifen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. von jeglicher Schwächung der Sicherheit des 5G-Standards abzusehen und anstatt dessen die Chancen eines sicheren 5G-Standards voranzutreiben.

    a. Hierzu soll sich die Bundesregierung in dem noch laufenden Standardisierungsprozess mit allen durch sie beteiligten Akteuren aktiv für ein höchstmögliches Maß an Sicherheit einsetzen. Hierzu zählt unter anderem der Einsatz für eine standardmäßige Ende-zu-Ende Verschlüsselung und die Ablehnung von Sicherheitslücken zur weiteren Möglichkeit der Nutzung von sogenannten IMSI-Catchern.

    b. Auf nationaler Ebene soll die Bundesregierung zum einen alle Maßnahmen unterlassen, die eine Schwächung der Sicherheit in der Anwendung der 5G-Technologie zur Folge hätten, und zum anderen proaktiv Maßnahmen ergreifen, um die Sicherheit in der Anwendung der 5G-Technologie zu stärken. So kann sie beispielsweise die Chance einer starken Übertragungsveschlüsselung dahingehend nutzen, ein wirksames Recht auf Verschlüsselung (wie bereits in den Anträgen der Fraktion der Freien Demokraten auf BT-Drs. 19/5764 und BT-Drs. 19/7698 gefordert) auch gesetzlich zu verankern.

2. die von von der Europäischen Kommission empfohlenen Maßnahmen zur "Cybersicherheit der 5G-Netze" (Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019) national umzusetzen. Hierunter fallen auf Grundlage der nationalen Risikobewertungen der Mitgliedstaaten insbesondere die folgenden Maßnahmen:

    a. Aktualisierung der für die 5G-Netze geltenden Sicherheitsanforderungen und Risikomanagementverfahren sowie der einschlägigen Verpflichtungen für Unternehmen, die öffentliche Kommunikationsnetze bereitstellen oder öffentlich zugängliche elektronische Kommunikationsdienste erbringen.

    b. Bedingungen im Hinblick auf den Schutz öffentlicher Netze gegen unbefugten Zugang an die Allgemeingenehmigung knüpfen und Unternehmen, die künftig an Verfahren zur Erteilung von Nutzungsrechten für Funkfrequenzen in 5G-Frequenzbändern teilnehmen, zur Einhaltung der Sicherheitsanforderungen für Netze verpflichten.

    c. Anbieter und Betreiber von 5G-Netzen dazu verpflichten, für die Sicherheit der sicher-heits-re-le-vante Netz- und System-kom-po-nenten zu sorgen, den zuständigen nationalen Behörden einschlägige Informationen über geplante Änderungen der elektronischen Kommunikationsnetze zur Verfügung zu stellen und spezifische Komponenten und IT-Systeme im Hinblick auf Sicherheit und Integrität vorab von einer nationalen Prüfstelle/einem Zertifizierungslabor testen zu lassen. Zu diesem Zweck soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständige Prüfstelle gesetzlich benannt werden und mit ausreichend personellen und finanziellen Ressourcen ausgestattet werden.

    d. Gemeinsame Durchführung von Sicherheitsüberprüfungen, wenn Unternehmen in mehreren Mitgliedstaaten Netzinfrastrukturen betreiben oder aufbauen. Die Agentur der EU für Cybersicherheit

(ENISA), Europol und das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) sollen Unterstützungsersuchen der Mitgliedstaaten in diesem Bereich Vorrang einräumen.

3. die Kooperation im Rahmen der Sicherheit der 5G-Netze auf europäischer Ebene zu intensivieren.

    a. Hierzu soll die Bundesregierung eine durch die Mitgliedstaaten und die jeweils zuständigen Einrichtungen auf Ebene der Mitgliedsstaaten und der Europäischen Union gemeinsam getragene Entwicklung einer koordinierten Risikobewertung auf Unionsebene vorantreiben, die auf den nationalen Risikobewertungen aufbaut.

    b. Außerdem soll sie bewährte Verfahren und mögliche gemeinsame Maßnahmen zur Minderung der Cybersicherheitsrisiken im Zusammenhang mit kritischen Infrastrukturen im Bereich der 5G-Netze durch die mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 eingesetzte Kooperationsgruppe abstimmen.

4. durch staatliche Behörden keine Produkte von chinesischen Unternehmen zu beziehen, deren Produkte Kern des Systems der uferlosen Massenüberwachung der Menschen in China sind. Die Bundesregierung muss den Wert deutlich machen, den es Freiheit und Bürgerrechten beimisst. Deshalb fordern wir die Bundesregierung konkret auf,

    a. bei sicherheitskritischer Infrastruktur, wie beispielsweise der 5G-Technologie, bereit zu sein sowohl national als auch durch das entsprechende Engagement auf europäischer Ebene auf die Nutzung chinesischer Technik zu verzichten, wie China auch bestimmte Bereiche von ausländischen Investitionen und Unternehmen ausnimmt.

    b. den Export von Überwachungstechnologien in Zeiten digitaler Vernetzung als kritischen Bereich zu betrachten; diese Technologien sind in autokratischen Staaten ein Mittel, die Freiheit von Meinungen und Medien einzuschränken und eine aktive Zivilgesellschaft zu unterdrücken. Europa braucht deshalb eine gemeinsame politische Linie für menschenrechtliche Standards in der Rüstungskontrolle, die auch neue Technologien einbeziehen, und einheitlich angewandte Verfahren.

Berlin, den 15. Oktober 2019

Christian Lindner und Fraktion