Deutscher Bundestag **Drucksache 19/16058**

19. Wahlperiode 18.12.2019

Antrag

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller, Marc Bernhard, Jürgen Braun, Siegbert Droese, Peter Felser, Dr. Götz Frömming, Wilhelm von Gottberg, Martin Hess, Dr. Heiko Heßenkemper, Jörn König, Dr. Rainer Kraft, Frank Magnitz, Jens Maier, Andreas Mrosek, Christoph Neumann, Tobias Matthias Peterka, Martin Reichardt, Dr. Robby Schlund, Uwe Schulz, Detlev Spangenberg, Dr. Christian Wirth und der Fraktion der AfD

Sicherstellung nationaler Souveränität im 5G-Mobilfunknetz

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Nicht nur die politische, sondern auch die technologische Souveränität Deutschlands ist ein wesentlicher Faktor für die Sicherheit und Integrität der nationalen Informations- und Kommunikationsinfrastruktur sowie sämtlicher Kritischer Infrastrukturen (KRITIS).

Das künftig aufzubauende 5G-Mobilfunknetz ist in besonderem Maße für die nationale Sicherheit und gesellschaftliche Prosperität relevant, da es darauf ausgelegt ist, milliardenfach Endgeräte mit dem Internet zu verbinden und damit Anwendungen wie autonomes Fahren, Industrie 4.0, Telemedizin oder Smart Grids zu ermöglichen. Damit wird die 5G-Infrastruktur zu einer wesentlichen technischen Voraussetzung zum Betrieb auch anderer Kritischer Infrastrukturen, wie etwa des Strom-, Gas-, Wasser- oder Straßenverkehrsnetzes.

Die zweifelsfreie Vertrauenswürdigkeit, Zuverlässigkeit und Leistungsfähigkeit von Ausrüstern der 5G-Infrastruktur ist aus technischen Gründen von besonderer Bedeutung, da die 5G-Systemkomponenten in sehr viel stärkerem Maße als bisher eine spezifische Kombination von Hard- und Software des jeweiligen Anbieters sind. Hinzu kommt die hohe Integration bei 5G von Zugangsnetz und Kernnetz, was das Zugriffsrisiko auf besonders sensible Daten im Kernnetz wesentlich erhöht.

Aufgrund der im Jahr 2019 durchgeführten nationalen Risikobewertung der 5G-Netzinfrastruktur kommt auch die Bundesregierung zu dem Schluss, dass „angesichts der Bedeutung von 5G für die künftige Wettbewerbsfähigkeit des Standortes die Technik, die beim Ausbau von 5G zum Einsatz kommt, höchste Sicherheitsstandards erfüllen muss. Sicherheitsbedenken müssen so weit wie möglich ausgeschlossen werden. Das gilt für die eingesetzte Hard- und Software gleichermaßen.“ (Ausschuss-Drucksache 19(23)053, S. 4)

Die Berücksichtigung von Unternehmen als Ausrüster der deutschen 5G-Infrastruktur, die durch Staaten kontrolliert werden, die nicht europäische Werte teilen, die als „Technologie- und System-Konkurrent“ (https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook_de.pdf, S.1) zu betrachten sind und die die „künftige Wettbewerbsfähigkeit des Standortes Deutschland“ (ebenda) unterminieren, kann nicht dazu geeignet sein, „Sicherheitsbedenken so weit wie möglich auszuschließen“ (ebenda).

So beruht die starke internationale Stellung des chinesischen Netzwerkausrüsters Huawei auf der protektionistischen Regulierung des chinesischen Marktes, auf dem 75 Prozent des Mobilfunkmarktes für heimische Technologieanbieter reserviert sind (www.tagesspiegel.de/politik/5g-mobilfunk-vertrauen-in-huawei-ist-riskant/23731840.html).

Im Dezember 2019 wurde ferner die vertrauliche sogenannte „3-5-2-Direktive“ des Generalbüros des Zentralkomitees der Kommunistischen Partei bekannt, die chinesische Behörden anweist, innerhalb von drei Jahren auf ausländische Computertechnologie oder Software zu verzichten (www.faz.net/aktuell/wirtschaft/digitec/chinas-behoerden-sollen-auslaendische-computer-austauschen-16526337.html).

Die großen Hoffnungen, die mit dem Beitritt der Volksrepublik China zur Welthandelsorganisation (WTO) im Jahr 2001 verbunden waren, wurden nicht nur durch diese Direktive weitestgehend enttäuscht (https://bdi.eu/artikel/news/china-in-der-wto/). So wurde insbesondere noch kein akzeptables Angebot für den Beitritt zum Government Procurement Agreement (GPA) vorgelegt, obwohl dies bereits mit der Aufnahme in die WTO vor 18 Jahren zugesagt wurde. Ferner befinden sich nach wie vor 99 der 100 größten börsennotierten Unternehmen in China mehrheitlich in Staatshand und mit der Selbst-Deklaration Chinas als „Entwicklungsland“ sind weiterhin viele Ausnahmen von den WTO-Regeln verbunden (ebenda).

Vertreter des Bundesnachrichtendienstes (BND) schilderten in der nichtöffentlichen Sitzung des Bundestagsausschusses Digitale Agenda vom 12. Dezember 2019 (www.bundestag.de/resource/blob/671910/70258f1a5bf543f4810e894238fa0eb4/19WP-44-data.pdf) die Absicht des chinesischen Staates, Informations- und Kommunikationstechnologie (IKT) als zentrales Instrument zur Umsetzung chinesischer Weltmacht-Ambitionen zu nutzen sowie die Rolle insbesondere des Unternehmens Huawei als „Speerspitze“. Huawei würde daher auch im Ausland von chinesischen Parteizellen „kontrolliert und gesteuert“ und sei „nicht vertrauenswürdig“.

Bereits im März 2019 urteilte das britische Huawei Cyber Security Evaluation Centre (HCSEC) in seinem 5. Jahresbericht u. a. (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf, S. 4–5):

- „Weitere signifikante technische Probleme wurden in den Entwicklungsprozessen von Huawei festgestellt, was zu neuen Risiken in den britischen IKT-Netzwerken führte“;
- „Wie bereits im Jahr 2018 berichtet, hat die Aufsichtsbehörde HCSEC weiterhin Probleme im Zusammenhang mit dem Ansatz von Huawei bei der Softwareentwicklung festgestellt, die das Risiko für britische IKT-Betreiber signifikant erhöht haben“;
- „Die Aufsichtsbehörde HCSEC kann daher nur begrenzt gewährleisten, dass alle Risiken für die nationale Sicherheit durch die Beteiligung von Huawei langfristig ausreichend gemindert werden können“.

Laut der Antwort der Bundesregierung (Bundestagsdrucksache 19/12959, S. 4) auf die Kleine Anfrage der AfD-Bundestagsfraktion zum „Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur“ (Bundestagsdrucksache 19/12269) ist das HCSEC der Bundesregierung seit dem Jahr 2010 bekannt.

Die Zulassung von potentiell nichtvertrauenswürdigen Netzwerkausrüstern auf der Grundlage einer Selbst-Kategorisierung als „vertrauenswürdig“ ist daher als nicht zielführend zu betrachten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

– sämtliche regulatorischen Maßnahmen zu treffen, die eine Nichtberücksichtigung von Netzwerkausrüstern von zweifelhafter Integrität, die die Sicherheit Kritischer Infrastrukturen, die Wettbewerbsfähigkeit des Standortes Deutschland sowie die technologische Souveränität Deutschlands gefährden, gewährleisten,
– bei der Umsetzung und Anwendung dieser Regularien, die Bewertung deutscher Sicherheitsbehörden zugrunde zu legen sowie
– mit geeigneten Fördermaßnahmen die europäische und nationale Souveränität im Bereich von Informations- und Kommunikationstechnologie auf absehbare Zeit deutlich zu stärken.

Berlin, den 13. Dezember 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Begründung

Laut § 109 des Telekommunikationsgesetzes (TKG) hat jeder Betreiber eines öffentlichen Telekommunikationsnetzes angemessene technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses und gegen Störungen zu treffen.

Aufgrund der technischen Komplexität des künftigen 5G-Mobilfunknetzes, aufgrund der strategischen Bedeutung der nationalen Informations- und Kommunikationsinfrastruktur sowie aufgrund der politischen Intentionen relevanter staatlicher Akteure ist nicht davon auszugehen, dass allein „technische Vorkehrungen“ für einen hinreichenden Schutz des öffentlichen Telekommunikationsnetzes ausreichend sind.

Zusätzliche rechtliche Vorkehrungen, wie Erklärungen der Vertrauenswürdigkeit oder no-spy-agreements, bieten ebenfalls keinen hinreichenden Schutz.

So wären solche Abkommen beispielsweise unvereinbar mit Artikel 7 des chinesischen Geheimdienstgesetzes aus dem Jahr 2017 (http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law), der vorschreibt, dass Organisationen und Bürger die nationale Geheimdienstarbeit unterstützen sollen und mit den Diensten kooperieren und dieses geheim halten sollen.

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.betrifft-gesetze.de
ISSN 0722-8333