

Antrag

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Ependiller, Stephan Brandner, Jürgen Braun, Siegbert Droese, Peter Felser, Albrecht Glaser, Wilhelm von Gottberg, Udo Theodor Hemmelgarn, Karsten Hilse, Martin Hohmann, Johannes Huber, Stefan Keuter, Jörn König, Rüdiger Lucassen, Jan Ralf Nolte, Gerold Otten, Tobias Matthias Peterka, Paul Viktor Podolay, Jürgen Pohl, Stephan Protschka, Dr. Robby Schlund, Jörg Schneider, Detlev Spangenberg, Dr. Dirk Spaniel, Dr. Harald Weyel, Dr. Christian Wirth und der Fraktion der AfD

IT-Sicherheitsgesetz 2.0 – Planungs- und Rechtssicherheit für Netzbetreiber herstellen

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Gerade in Zeiten der Corona-Pandemie und der daraus resultierenden sozialen Distanzierung ist eine vollständig ausgebaute und gut funktionierende digitale Infrastruktur unumgänglich.

Die deutschen Netzbetreiber bilanzieren vor allem im Pandemie-Jahr 2020, dass der Ausbau des 5G-Netzes teilweise schneller stattgefunden und vorangetrieben werden konnte als geplant. Nach Angaben verschiedener Netzbetreiber in Deutschland sollen zum Anfang des Jahres 2021 bis zu zwei Drittel der Bevölkerung mit der fünften Generation des Mobilfunkstandards versorgt werden können. Mehrere Städte in Deutschland werden demnach schon mit 5G versorgt. Die Netzbetreiber können vielerorts auf die schon auf bestehende 4G-Masten zurückgreifen und auf 5G um- oder nachrüsten. Laut der Deutschen Telekom AG befinden sich bereits rund 45.000 5G-Funkmasten in Betrieb (www.tagesschau.de/wirtschaft/technologie/5g-ausbau-in-deutschland-101.html).

Bei zunehmender Digitalisierung von Verwaltung, Wirtschaft und Gesellschaft kommt vor allem der IT- und Cyber-Sicherheit eine übergeordnete Rolle zu. Für die regulatorische Umsetzung dieser hohen digitalen Sicherheitsanforderungen hat die Bundesregierung nach monatelangem Zögern den Entwurf eines IT-Sicherheitsgesetzes 2.0 vorgelegt. Darin bleiben jedoch zentrale Fragen zu entstehenden Kosten sowie zu Planungs-, Investitions- und Rechtssicherheit bezüglich der Verwendung von Netzwerkkomponenten chinesischer Netzwerkausrüster genau so offen, wie Fragen nach dem Rückgriff auf das Bestandsnetz (www.telefonica.de/news/corporate/2020/12/it-sicherheitsgesetz-telekommunikationsbranche-braucht-investitionssicherheit.html). Dies

wird insbesondere daran sichtbar, dass die Netzbetreiber, nach Ansicht der Antragsteller, ein erhöhtes Risiko eingehen, wenn weiterhin Netzwerkkomponenten chinesischer Hersteller Verwendung finden oder eingesetzt werden. Theoretisch könnte, so die Annahme der Antragsteller, die Verwendung solcher Netzwerkkomponenten aus undemokratischen Ländern zu jedem Zeitpunkt – auch zukünftig – unter Verbot gestellt werden (§ 9b des IT-Sicherheitsgesetzes, Untersagung des Einsatzes kritischer Komponenten).

Das unter § 9b des IT-Sicherheitsgesetz-Entwurfs beschriebene Verfahren zur Prüfung von Restrisiken sowie der Vertrauenswürdigkeit von Herstellern kritischer Komponenten ist, nach Ansicht der Antragsteller, nicht geeignet, zügig eine klare Rechts- und Planungssicherheit für deutsche Mobilfunknetzbetreiber herzustellen. Mit dieser unkonkreten Positionierung der Bundesregierung im IT-Sicherheitsgesetz 2.0 zum Schutz der kritischen Infrastruktur wurde lediglich ein Kompromiss geschlossen, der die Netzbetreiber mit offenen Fragen im Hinblick auf Netzwerkkomponenten und -ausrüster aus undemokratischen Ländern alleine lässt. Es wurde von der Bundesregierung versäumt, eine klare und endgültige politische Entscheidung darüber zu treffen, ob staatsnahe Netzwerksausrüster aus undemokratischen Ländern am Ausbau kritischen 5G-Infrastruktur beteiligt werden dürfen. Die Netzbetreiber müssen eine entsprechende Entscheidung der Behörde (Untersagungsvorbehalt) abwarten, bevor der Einsatz von kritischen Komponenten von Netzwerksausrüstern zum Beispiel aus China gestattet wird.

Mit zunehmender informationstechnischer Komplexität der eingesetzten kritischen Komponenten bleibt ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen von Sicherheitslücken) beim Hersteller selbst oder in der weiteren Lieferkette und nicht beim Betreiber des Netzwerkes oder bei den Behörden. Daher und aufgrund der zu erwartenden stetigen Updates (Soft- oder Firmware) bieten weder eine Komponentenzertifizierung, noch hohe technische Sicherheitsanforderungen eine ausreichende Sicherheit dahingehend, dass die Hersteller keine missbräuchlichen Zugriffsmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen (www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/entwurf-zweites-it-sicherheitsgesetz.pdf?__blob=publicationFile&v=1).

Ein maximaler Schutz hoheitlicher, personenbezogener, wissenschaftlicher und wirtschaftlich verwertbarer Daten und der damit einhergehenden digitalen Souveränität ist von übergeordneter Bedeutung. Insbesondere Softwarekomponenten bilden einen zentralen Bestandteil der 5G-Netzwerke. Die Funktionalität dieser Komponenten kann nach einem abgeschlossenen Zulassungsverfahren zügig über Updates angepasst werden und würde sich damit der Kontrolle der Behörden entziehen. Dieser zentrale Aspekt moderner Telekommunikationsnetze wird im vorliegenden Entwurf nicht ausreichend berücksichtigt und gewürdigt. Der vorgelegte Gesetzentwurf ist daher, nach Ansicht der Fragesteller, nicht geeignet, einen schnellen und rechtssicheren Ausbau der 5G-Netze durch die Mobilfunknetzbetreiber zu gewährleisten.

II. Der Deutsche Bundestag fordert die Bundesregierung daher auf,

- im Rahmen eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) eine klare und endgültige politische Entscheidung darüber zu treffen, ob staatsnahe Netzwerksausrüster aus undemokratischen Ländern am Ausbau kritischen 5G-Infrastruktur beteiligt werden dürfen,

- die Rechts- und Planungssicherheit für Mobilfunknetzbetreiber dahingehend herzustellen, dass für die Folgen eines möglichen Ausschlusses von Herstellern kritischer Komponenten eine hinreichende Absicherung für die Mobilfunkbetreiber in Form von entsprechenden Kompensationsregelungen im Gesetz mit aufgenommen wird,
- Überleitungsvorschriften im IT-SiG 2.0 aufzunehmen, die festlegen, dass der Regulierungsmechanismus sowie die Folgen des § 9b des IT-Sicherheitsgesetzes 2.0 nur für Komponenten angewendet werden, deren Nutzung zukünftig beim BMI angezeigt werden. Eine Rückwirkung auf Bestandsnetze muss aus Gründen des Investitions- und Vertrauensschutzes ausgeschlossen werden.

Berlin, den 22. Januar 2021

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Begründung

Seit fast zwei Jahren diskutiert der Bundestag über die Frage der Zulassung von Netzwerkausrüstern bei Ausbau des 5G-Netzes, deren Vertrauenswürdigkeit zumindest fragwürdig ist. Insbesondere Hersteller aus undemokratischen Ländern sind dabei in den Blickpunkt geraten. Die Volksrepublik China besitzt mit ihren Herstellern Huawei und ZTE zwei Hersteller, deren Technik weltweit Verwendung finden. Als problematisch wird die Nähe dieser Unternehmen zum chinesischen Militär, sowie der kommunistischen Partei angesehen. Es besteht die Gefahr, dass die Unternehmen auf Druck der chinesischen Regierung ihre Netzwerkkomponenten für Spionage und Sabotage Eingriffe zur Verfügung stellen könnten. Faktisch sind chinesische Unternehmen gesetzlich dazu verpflichtet, mit der chinesischen Regierung zusammenzuarbeiten. Unternehmen die sich der Zusammenarbeit widersetzen, oder zumindest nicht ganz im Sinne der kommunistischen Partei arbeiten, werden durch die Regierung massiv unter Druck gesetzt. So geriet das Unternehmen Alibaba, eines der wertvollsten Unternehmen der Welt und Chinas größter Onlinehändler, in das Visier der kommunistischen Regierung, nach dem sich sein Gründer Jack Ma bei einem öffentlichen Auftritt im letzten Oktober kritisch zum chinesischen Finanzsystem äußerte. Der für November geplante Börsengang wurde kurzfristig auf Druck der kommunistischen Staatsführung abgesagt (www.tagesschau.de/wirtschaft/alibaba-ermittlungen-101.html). Jack Ma wurde nach seinem Auftritt im Oktober mehrere Monate nicht mehr in der Öffentlichkeit gesehen.

Die Vertrauenswürdigkeit der 5G-Netzwerkausrüster ist unerlässlich für die nationale Sicherheit und digitale Souveränität der Bundesrepublik Deutschland und Europas. Daher ist es zwingend erforderlich, dass ausschließlich zweifelsfrei vertrauenswürdige Hersteller zum Einsatz kommen. Der Bundesnachrichtendienst sowie mehrere Sicherheitsdienste ziehen die Vertrauenswürdigkeit chinesische Hersteller jedoch in Zweifel. Mehrere europäische Länder sowie weltweite Bündnispartner haben den Einsatz chinesische Technologie beim Ausbau ihres 5G-Netzes bereits ausgeschlossen.

Die Bundesregierung hat sich bisher auf keine klare Position festgelegt. Auch der nun vorgelegte Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme enthält keine klare Positionierung diesbezüglich.

Der Ausbau des 5G-Netzes schreitet jedoch bereits voran und sollte keinesfalls durch fehlende Rechtssicherheit verzögert werden. Diese fehlende Planungs- und Rechtssicherheit wird durch die Mobilfunkunternehmen beklagt. Das Unternehmen Telefonica kritisierte den vorgelegten Gesetzentwurf wie folgt: „Die Folgen eines möglichen Ausschlusses sind nicht geregelt, es gibt keine ausreichende Rechts- und Planungssicherheit und es droht ein Rückgriff auf Bestandsnetze“ (www.tagesschau.de/wirtschaft/technologie/5g-ausbau-in-deutschland-101.html). Ähnlich äußerte sich die Deutsche Telekom.

Die Bundesregierung weist im vorliegenden Gesetzentwurf selbst darauf hin, dass weder eine Komponentenzertifizierung, noch hohe technische Sicherheitsanforderungen eine ausreichende Sicherheit dahingehend, dass die

Hersteller keine missbräuchlichen Zugriffsmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen (www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=2 – Seite 100).

Um eine abschließende Planungs- und Rechtssicherheit herzustellen ist es daher notwendig, dass der vorgelegte Gesetzesentwurf dahingehend geändert wird, dass er eine klare politische Entscheidung darüber trifft, ob Hersteller aus undemokratischen Ländern grundsätzlich für den Ausbau des 5G-Netzes zugelassen werden (www.basecamp.digital/it-sicherheitsgesetz-lueckenhafte-regeln-sollen-fuer-mehr-sicherheit-sorgen/).