Deutscher Bundestag **Drucksache 19/7723**

19. Wahlperiode 13.02.2019

Antrag

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller, Dr. Götz Frömming, Marc Bernhard, Stephan Brandner, Jürgen Braun, Marcus Bühl, Matthias Büttner, Tino Chrupalla, Peter Felser, Dietmar Friedhoff, Wilhelm von Gottberg, Armin-Paulus Hampel, Verena Hartmann, Martin Hebner, Lars Herrmann, Martin Hess, Karsten Hilse, Nicole Höchst, Martin Hohmann, Dr. Marc Jongen, Jens Kestner, Jörn König, Dr. Rainer Kraft, Andreas Mrosek, Christoph Neumann, Ulrich Oehme, Gerold Otten, Dr. Robby Schlund, Thomas Seitz, Detlev Spangenberg, Dr. Dirk Spaniel, Beatrix von Storch, Dr. Harald Weyel, Dr. Christian Wirth und der Fraktion der AfD

Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Der chinesische Netzwerkausrüster Huawei wurde bislang von unseren befreundeten Demokratien Großbritannien, Neuseeland, Australien und den USA als Zulieferer beim Aufbau des nationalen 5G-Netzes ausgeschlossen. Dies wird in der Regel mit Gründen der nationalen Sicherheit begründet, so z.B. durch das Government Communications Security Bureau (GCSB) in Neuseeland oder das Huawei Cyber Security Evaluation Centre (HCSEC) des britischen Geheimdienstes GCHQ (https://www.tagesspiegel.de/politik/5g-mobilfunk-vertrauen-in-huawei-ist-riskant/23731840.html). Auch die EU-Kommission prüft Medienberichten zufolge den Ausschluss von außereuropäischen Netzwerkausrüstern (n-tv, 31.1.2019).

British Telecom hat damit begonnen, alle Produkte von Huawei auch aus dem Kernnetz der schon bestehenden 3G- und 4G-Infrastruktur durch Produkte anderer Hersteller zu ersetzen (https://www.theguardian.com/technology/2018/dec/05/bt-removing-huawei-equipment-from-parts-of-4g-network). Vodafone Deutschland wird alle Huawei-Komponenten seines 3G- und 4G-Kernnetzes bis Ende 2020 gegen Nokia-Produkte austauschen (http://www.spiegel.de/politik/deutschland/huawei-minister-sollen-bei-5g-geheimtreffen-ueber-chinesischen-konzern-beraten-a-1251768.html). Die polnische Regierung nahm eine Spionage-Anklage gegen einen Mitarbeiter des Huawei-Konzerns in Polen zum Anlass, ein gemeinsames Vorgehen der Nato und der EU gegen Huawei zu

fordern (https://www.theguardian.com/world/2019/jan/12/huawei-sacks-chinese-worker-accused-of-spying-in-poland-wang-weijing).

Weder in Großbritannien noch in Deutschland oder Australien gibt es Zulieferer, die unmittelbar von einem Ausschluss ausländischer Anbieter wirtschaftlich profitieren, da alternative Netzwerktechnologie insbesondere von den europäischen Firmen Nokia und Ericsson angeboten wird. Dahingegen beruht die starke internationale Stellung von Huawei auf der protektionistischen Regulierung des chinesischen Marktes, auf dem 75 Prozent des Mobilfunkmarktes für heimische Technologieanbieter reserviert ist (https://www.tagesspiegel.de/politik/5g-mobilfunk-vertrauen-in-huawei-ist-riskant/23731840.html).

Sicherheitsrelevante Aspekte bei dem Aufbau des 5G-Netzes in Deutschland betreffen nicht allein Datenschutzfragen oder das Ausspionieren von Geschäftsgeheimnissen über die Fernwartungszugänge der Netzwerkausrüster, sondern die Integrität des gesamten Telekommunikationsnetzes, das für unsere Wirtschaft und auch unsere Gesellschaft buchstäblich überlebenswichtig sein kann. Mit Hilfe eines sogenannten „Kill Switches“ ist es Netzwerkausrüstern möglich, die Betriebssicherheit des 5G-Netzes erheblich zu gefährden, wenn nicht gar das Netz komplett abzuschalten (https://www.tagesschau.de/wirtschaft/huawei-telekommunikation-netzausbau-101.html).

Es ist zwar aufgrund der potenziellen politischen, wirtschaftlichen und ggf. auch militärischen Vergeltungsmaßnahmen nicht davon auszugehen, dass einzelne Unternehmen aus eigenem Ermessen oder in staatlichem Auftrag mit Hilfe eines „Kill Switches“ Produktionsprozesse in der Industrie oder die Steuerung der Energieversorgung unmittelbar zum Erliegen bringen. Es erscheint jedoch durchaus denkbar, dass, wie bei der Anwendung des sogenannten „Stuxnet“-Virus im Jahr 2010 bereits erfolgt, in industriellen Produktionsprozessen durch Störungen der Verfügbarkeit des 5G-Netzwerks oder durch Steuerbefehle aus dem Kernnetz unbemerkt Fehlfunktionen ausgelöst werden, die langfristig zu einer Selbst-Zerstörung der entsprechenden Anlagen führen. Bei einer umfassenden Vernetzung von Produktionsanlagen im Sinne des Industrie 4.0-Prinzips hätte ein solches Szenario unkalkulierbare betriebs- und volkswirtschaftliche Schäden zur Folge.

Die Überprüfungen der Netzwerk-Technologie des Huawei-Konzerns durch das BSI in dem im November 2018 eingerichteten Security Innovation Lab sind nach Ansicht von Experten nicht hinreichend und können prinzipiell auch keine prospektiven Gefährdungsaussagen z. B. im Hinblick auf künftige Software-Updates treffen (https://www.tagesschau.de/wirtschaft/huawei-telekommunikation-netzausbau-101.html). Dazu hatte das GCHQ bereits im Jahr 2018 die Aussage getroffen, man habe zwar den von Huawei zur Verfügung gestellten Programmcode geprüft, könne aber keine zuverlässigen Aussagen über jenen Programmcode treffen, der in den Produkten von Huawei tatsächlich zur Anwendung kommt.

Die einmalige Offenlegung von Programmcodes oder die Zertifizierung von Netzwerkkomponenten sind für die Gewährleistung der digitalen Souveränität ebenso wenig hinreichend wie sogenannte „No-spy-Klauseln“ in Beschaffungsverträgen.

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

Damit unvereinbar ist jedoch 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.

Es ist aus Gründen der nationalen Sicherheit wie auch aus wirtschaftlichen und gesellschaftlichen Gründen nicht hinnehmbar, dass von ausländischen Regierungen, insbesondere solchen, die nicht europäische Werte teilen, kontrollierte Unternehmen bei dem Aufbau der nationalen 5G-Infrastruktur in wesentlichem Maße Berücksichtigung finden und damit die Integrität dieser Infrastruktur dauerhaft gefährden. Die im Koalitionsvertrag vereinbarte und als „besonders wichtig erachtete“ digitale Souveränität ist damit nicht zu gewährleisten.

Der Anspruch Deutschlands muss es vielmehr sein, weltweiter Leitmarkt bei vertrauenswürdiger Hard- und Software zu sein.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

- eine Einstufung des 5G-Netzes als Kritische Infrastruktur im Sinne des §5 der Kritisverordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-KritisV) vorzunehmen und dafür den Regelschwellenwert von 500.000 versorgten Personen erneut zu prüfen und ggf. nach unten zu korrigieren,
- die Sicherheitsanforderungen des Telekommunikationsgesetzes (TKG) an die Kritikalität des 5G-Netzes sowie an aktualisierte Gefährdungsanalysen anzupassen,
- das Gesetz für Cybersicherheit aus dem Jahr 2016 auf die 5G-Infrastruktur auszuweiten,
- in dem angekündigten IT-Sicherheitsgesetz 2.0 den zunehmend fremdstaatlich initiierten Sicherheitsrisiken im Cyberraum Rechnung zu tragen,
- entsprechende Gesetzesänderungen im Geist der 2017 verabschiedeten Neuerungen im Außenwirtschaftsgesetz vorzunehmen, nach denen Investitionen verboten werden können, die die öffentliche Ordnung und Sicherheit gefährden,
- eine Beweislastumkehr einzuführen, nach der Netzwerkausrüster ihre staatliche Unabhängigkeit erklären und plausibilisieren müssen, um zu Ausschreibungen zugelassen zu werden,
- die bestehenden Möglichkeiten der Ende-zu-Ende-Verschlüsselung auf Anwendungsebene zu bewahren und auszubauen, da sie ein hohes Maß an Sicherheit gewährleisten und für die Nutzer ferner transparent und nachvollziehbar sind,
- das BSI mit den entsprechenden Ressourcen auszustatten, sämtliche Programmecode-Updates vor deren Installation umfassend zu prüfen und zu zertifizieren,
- im Bereich der noch verbleibenden Standardisierung von 5G, insbesondere im Rahmen des Third Generation Partnership Projects (3GPP), bis zum Jahr 2020 zusätzliche öffentliche Mittel zu veranschlagen, um die Wahrnehmung deutscher Interessen in internationalen Standardisierungsgremien insbesondere im Bereich der Netzwerksicherheit zu gewährleisten,
- lediglich Unternehmen mit Hauptsitz in demokratischen Ländern Europas zu Ausschreibungen zuzulassen, die damit in besonderer Weise der Kontrolle durch europäische Institutionen unterstehen und damit auch

langfristig, bei einer möglichen künftigen Marktreife auch von nicht-asiatischen Netzwerkausrüstern, eine Gefährdung der nationalen Sicherheit und der Integrität des 5G-Netzes zu minimieren.

Berlin, den 8. Februar 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

Begründung

Das künftig aufzubauende 5G-Netz ist in besonderem Maße für die nationale Sicherheit relevant, da es explizit darauf ausgelegt ist, im Sinne der Vision eines „Internets der Dinge“ (IoT) milliardenfach Endgeräte mit dem Internet zu verbinden und damit Anwendungen wie autonomes Fahren, Industrie 4.0, Smart Home oder Smart Grid 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 Integrität von potenziellen Netzwerkausrüstern für das künftige 5G-Netz ist aus technischen Gründen umso bedeutender, da die 5G-Systemkomponenten in sehr viel stärkerem Maße als bei den bisherigen xG-Komponenten eine spezifische Kombination von Hard- und Software des jeweiligen Anbieters sind. Dies ergibt sich aus der stark Software-basierten Auslegung des 5G-Netzes, um es dynamisch den jeweiligen Nutzungsanforderungen anzupassen.

Ein weiterer technischer Grund für besondere Sicherheitsanforderungen an Netzwerkausrüster ist die hohe Integration bei 5G von Zugangsnetz und Kernnetz als Bestandteile eines jeden Mobilfunk-Netzes. Ist es bei 3G- oder 4G-Netzen, wie im Falle British Telecom, noch möglich, Ausrüster vom Kernnetz auszuschließen, im Zugangssetz jedoch noch weiter einzusetzen, so ist diese Aufteilung im 5G-Netz nicht mehr möglich. Bereits über das Zugangsnetz bekommt ein Netzwerkausrüster weitreichenden Zugriff zu dem Kernnetz.

Die bisherigen Prüfungen des BSI von Programmcodes („code inspections“) der Produkte der Firmen Huawei und auch Cisco können keine dauerhaft gültigen Aussagen über die Integrität der geprüften Komponenten treffen, da die Hersteller über den Fernwartungszugang mit Hilfe von Software-updates jederzeit die Möglichkeit haben, die Programmcodes zu ändern. Es wäre daher Aufgabe des BSI, jede Änderung eines Programmcodes vor dessen Installation zu prüfen, falls dies technisch und organisatorisch überhaupt möglich ist. Eine solche kontinuierliche Prüfung wird in Deutschland derzeit nicht durchgeführt.

Das Abgreifen von Kommunikationsinhalten über den Fernwartungszugang zu Spionagezwecken wäre zwar auch durch eine In-situ-Beobachtung des erfolgten Datenverkehrs sichtbar. Aufgrund der vermutlich in diesem Fall geringen, da spezifisch gefilterten Datenvolumina sowie deren Verschlüsselung ist eine solche Art der Spionage jedoch nur schwer feststellbar und im Nachhinein auch nicht mehr heilbar.