**Deutscher Bundestag** **Drucksache 19/9621**

**19. Wahlperiode** 24.04.2019



# Antwort

## der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD**
**– Drucksache 19/8650 –**

## Sicherstellung der technischen Integrität der künftigen 5G-Mobilfunkinfrastruktur

Vorbemerkung der Fragesteller

Laut Medienberichten gab es Anfang Februar 2019 (www.handelsblatt.com/politik/deutschland/5g-ausbau-bnd-und-auswaertiges-amt-warnen-vor-chinas-macht-ueber-huawei/23991388.html) Treffen der außen-, wirtschafts- und digitalpolitischen Obleute des Deutschen Bundestages mit verschiedenen Bundesbehörden, darunter insbesondere der Bundesnachrichtendienst (BND), in denen aktuelle Erkenntnisse über sicherheitsrelevante Informationen über den Aufbau des künftigen 5G-Mobilfunknetzes in Deutschland präsentiert wurden.

Weitere Informationen sollen Regierungsbeamten, Parlamentariern und ausgewählten Empfängern in Form eines Papiers des Mercator Institute for China Studies (MERICS) vorgelegt worden sein (www.handelsblatt.com/politik/deutschland/huawei-konflikt-studie-zu-5g-warnt-vor-chinesischer-netzwerk technologie/24024110.html).

1. Liegen der Bundesregierung, insbesondere durch Informationen des BND oder auch anderer nachgeordneter Behörden, Informationen über einen konkreten Sicherheitsvorfall („smoking gun“) mit Huawei-Hardware vor?

Der Bundesregierung liegen keine Informationen über einen konkreten Sicherheitsvorfall mit Huawei-Hardware vor.

2. Liegen dem Bundesnachrichtendienst nähere Informationen zu den NSA-Operationen „Parody Blowup“ oder „Shotgiant“ aus den Jahren 2006 und 2009 vor, die Huawei als „einzigartige Bedrohung“ beschreiben (www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spionageverdacht-konzern)?

Dem BND liegen keine über die Presseberichterstattung hinausgehenden Informationen zu den NSA-Operationen „Parody Blowup“ und „Shotgiant“ aus den Jahren 2006 und 2009 vor.

---

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 18. April 2019 übermittelt.*

*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

3. Welche Schlussfolgerungen zieht die Bundesregierung aus der Einschätzung des Mercator Institute for China Studies (MERICS), dass sich weder Huawei noch andere chinesische Konzerne dem Einfluss des chinesischen Staates, insbesondere auf Basis des am 1. Mai 2015 in Kraft getretenen Staatssicherheitsgesetzes, aus Gründen der Nationalen Sicherheit entziehen können (www.golem.de/news/huawei-wartungsschnittstellen-sind-keine-hintertueren-1902-139554.html)?

4. Welche Schlussfolgerungen zieht die Bundesregierung aus der Einschätzung des Mercator Institute for China Studies (MERICS), dass auch die tatsächliche Rechts- und Verwaltungspraxis in China nicht dafür spricht, im Bereich kritische Infrastruktur und Daten vertrauensvoll mit chinesischen Unternehmen zusammenarbeiten zu können (www.golem.de/news/huawei-wartungsschnittstellen-sind-keine-hintertueren-1902-139554.html)?

Die Fragen 3 und 4 werden gemeinsam beantwortet.

Bei der Definition von Sicherheitsanforderungen für Telekommunikationsnetze lässt die Bundesregierung alle sicherheitsrelevanten Informationen einfließen.

Der Bundesregierung sind die Gesetzgebung sowie Rechts- und Verwaltungspraxis der Volksrepublik China bekannt.

5. Priorisiert die Bundesregierung entweder einen schnellen Ausbau des 5G-Mobilfunknetzes in Deutschland oder die Verwendung sicherer Soft- und Hardwarekomponenten, welche Gründe legt die Bundesregierung ihrer Entscheidung zugrunde, und welche Folgerungen ergeben sich aus dieser Priorisierung für die Bundesregierung?

Die Bundesregierung erwartet, dass die Basisstationen der fünften Generation (5G) zunächst auf den Netzen der vierten Generation aufbauen werden (sogenannte 5G Non-Standalone-Netze) und die Mobilfunknetzbetreiber den Ausbau zu Netzen mit vollem Leistungsumfang (sogenannte 5G Standalone-Netze) bedarfsorientiert über mehrere Jahre vornehmen werden. Zudem haben die Mobilfunknetzbetreiber bereits heute auf Grundlage von § 109 Absatz 4 des Telekommunikationsgesetzes (TKG) Sicherheitskonzepte zu erstellen, um Gefährdungen wirksam zu begegnen. Grundlage für die Sicherheitskonzepte ist ein Katalog von Sicherheitsanforderungen, den die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt.

Am 7. März 2019 hat die Bundesnetzagentur die Eckpunkte für eine Erweiterung des Katalogs an Sicherheitsanforderungen für den Betrieb von Telekommunikationsnetzen im Hinblick auf den Ausbau der 5G-Netze veröffentlicht (www.bundesnetzagentur.de/sicherheitsanforderungen). Die Netzbetreiber müssen im Rahmen ihrer Sicherheitskonzepte zukünftig die erweiterten Sicherheitsanforderungen erfüllen.

6. Mit welchen zusätzlichen Kosten für den Aufbau der 5G-Infrastruktur rechnet die Bundesregierung bei einem Ausschluss von Huawei und dem Ersatz von Huawei-Produkten durch andere Hersteller?

Zu den Kosten des 5G-Netzausbaus kann die Bundesregierung keine belastbaren Aussagen treffen.

7. Nach welchen spezifischen Kriterien des Katalogs von Sicherheitsanforderungen nach § 109 des Telekommunikationsgesetzes (TKG) beabsichtigt die Bundesregierung die geplante Vertrauenswürdigkeitsprüfung von Hersteller-„Ländern“ durchzuführen, und welche weiteren Kriterien sollen im Rahmen der geplanten Gesetzesänderung des TKG (www.golem.de/news/tkg-aenderung-regierung-plant-angeblich-knebelgesetz-fuer-huawei-1902-139360.html) dazu noch in den § 109 aufgenommen werden?

Betreiber von öffentlichen Telekommunikationsnetzen sind verpflichtet, technische Schutzmaßnahmen nach § 109 TKG umzusetzen. Hierzu hat die Bundesnetzagentur in Abstimmung mit dem BSI erste Eckpunkte für eine Überarbeitung des Katalogs an Sicherheitsanforderungen erstellt und veröffentlicht. Diese sehen eine Überprüfung von kritischen Kernkomponenten von beim BSI anerkannten Prüfstellen und eine Zertifizierung durch das BSI vor. Details zur Ausgestaltung sind in der Bearbeitung.

Im Zuge des Aufbaus von 5G-Netzen ist auch geplant, im Rahmen der laufenden Novellierung des Telekommunikationsgesetzes § 109 TKG zu überarbeiten und um zusätzliche verbindliche Sicherheitsanforderungen zu ergänzen.

Ferner ist eine Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik, mit Regelungen für Kritische Infrastrukturen und die Vertrauenswürdigkeit von Komponenten beabsichtigt, die in kritischen Infrastrukturen zum Einsatz kommen. Kritische Kernkomponenten, die in Kritischen Infrastrukturen eingesetzt werden, sollen nur von vertrauenswürdigen Lieferanten/Herstellern bezogen werden dürfen. Diese Verpflichtung soll für die gesamte Lieferkette gelten. Der Nachweis der Vertrauenswürdigkeit wird im Rahmen der Zertifizierung nach den Vorgaben des § 9 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik zu erbringen sein.

8. In welcher Form soll die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung nach einer Beweislastumkehr für Netzwerkausrüster gesetzgeberisch und exekutiv umgesetzt werden, und bis wann?

Um konkrete Anforderungen des zukünftigen Katalogs an Sicherheitsanforderungen nach § 109 Absatz 6 TKG auch auf Gesetzesebene abzusichern, plant die Bundesregierung im Rahmen der laufenden Novelle eine entsprechende Änderung des § 109 TKG.

9. Werden derzeit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder andere Bundesbehörden im Rahmen von Zertifizierungsverfahren kontinuierliche und vollumfängliche Prüfungen sämtlicher Hard- und Software-Updates für 2G-, 3G- und 4G-Netze durchgeführt?

   Wenn nein, warum nicht?

Es wurden durch das BSI keine kontinuierlichen und vollumfänglichen Prüfungen von 2G-, 3G- und 4G-Netzwerkkomponenten durchgeführt, da das BSI hierfür keine gesetzliche Aufgabe hat. Allgemeine Netzwerkkomponenten, die auch in 2G-, 3G-, 4G- und 5G-Infrastrukturen eingesetzt werden, werden auf Herstellerantrag nach den Common Criteria zertifiziert.

Auch die Bundesnetzagentur führt Prüfungen der beschriebenen Art derzeit nicht durch. Der Bundesnetzagentur sind vielmehr von Betreibern öffentlicher Telekommunikationsnetze und ggf. auch von Erbringern öffentlich zugänglicher Te-

lekommunikationsdienste nach § 109 Absatz 4 TKG bestimmte Sicherheitskonzepte über technische Schutzmaßnahmen vorzulegen, deren Umsetzung von der Bundesnetzagentur regelmäßig geprüft wird.

10. Sind solche kontinuierlichen und vollumfänglichen Prüfungen sämtlicher Hard- und Software-Updates im Rahmen von Zertifizierungsverfahren auch für das 5G-Netz geplant?

Es wird auf die Antwort zu Frage 7 verwiesen.

11. Hält die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, das „BSI mit entsprechenden Ressourcen auszustatten, sämtliche Programmecode-Updates vor deren Installation umfassend zu prüfen und zu zertifizieren“, für realistisch und zielführend, und wird die Bundesregierung diese Forderung umsetzen?

Grundsätzlich ist es möglich, bei ausreichender Ressourcenlage sicherheitstechnisch relevante Updates kritischer Systemkomponenten vor der Installation zu prüfen. Zudem wird auf die Antwort zu Frage 7 verwiesen, wonach die Heranziehung von beim BSI anerkannten Prüfstellen geplant wird.

12. Wie bewertet die Bundesregierung die Aussage des BSI-Präsidenten Arne Schönbohm, das BSI könne jedes einzelne von Huawei verbaute Gerät und jedes Software-Update vor Inbetriebnahme prüfen, (www.zeit.de/2019/09/huawei-mobiles-internet-5g-china-spionageverdacht-konzern) im Hinblick auf ihre Umsetzbarkeit?

Es wird auf die Antwort zu Frage 11 verwiesen.

13. Wie viele von Huawei verbaute Geräte und wie viele Software-Updates pro Zeiteinheit legt BSI-Präsident Arne Schönbohm dieser Aussage zugrunde?

Es wird auf die Antwort zu Frage 11 verwiesen.

14. Welche personellen (bitte Anzahl der Personalstellen in Vollzeitäquivalenten angeben), technischen (bitte Anzahl Laborgeräte, Server etc. angeben), finanziellen (bitte in Tausend Euro angeben) und organisatorischen (bitte Konzepte zur Organisationsgestaltung, z. B. in Form einer besonderen Aufbauorganisation – BAO –, Verantwortlichkeiten, Prüfabläufen etc. angeben) Voraussetzungen sind für die Umsetzung der von BSI-Präsident Schönbohm angekündigten Huawei-Prüfungen erforderlich, und bis wann, und in welchem Aufwuchszeitraum (bitte in Personenmonaten angeben) können diese Voraussetzungen geschaffen werden?

Die Planungen des BSI bezüglich Produktprüfungen orientieren sich an den von der BNetzA veröffentlichten Eckpunkten zum Katalog nach §109 TKG (www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2019/20190307_ITsicherheitskatalog.html?nn=265778). Rahmenbedingungen, wie beispielsweise die Definition des Umfangs der zu prüfenden Produktklassen, sind noch nicht in einer zur Beantwortung dieser Frage notwendigen Detailtiefe festgelegt worden.

15. Sieht die Bundesregierung Handlungsbedarf hinsichtlich einer EU-rechtlichen Harmonisierung des § 109 TKG, um eine einheitliche Rechtsgrundlage für ein konsolidiertes europäisches Vorgehen zum Schutz kritischer Telekommunikationsinfrastrukturen zu schaffen?

    Wenn nein, warum nicht?

Zur Sicherheit und Integrität von Netzen und Diensten bestehen mit den Artikeln 13a und 13b der Richtlinie 2009/140/EG zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und –dienste Harmonisierungsvorgaben auf EU-Ebene.

Diese Vorgaben wurden mit § 109 Absatz 4, 5 und 7 TKG in nationales Recht umgesetzt (Bundestagsdrucksache 17/5707, S. 83). § 109 TKG leitet sich daher bereits jetzt in wesentlichen Teilen aus EU-Vorgaben ab.

Mit der anstehenden Umsetzung der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation (hier v. a. Artikel 40 und 41) wird das TKG entsprechend den neuen Harmonisierungsvorgaben angepasst werden.

Die Bundesnetzagentur ist zudem initiativ, um die diesbezügliche inhaltliche Ausgestaltung mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und den anderen Mitgliedstaaten und damit eine möglichst harmonisierte Anwendung voranzutreiben.

16. Welche Möglichkeiten sieht die Bundesregierung, EU-Champions als Hersteller von Hard- und Softwarekomponenten von KRITIS-Infrastruktur oder die Ansiedlung von Produktionskapazitäten außereuropäischer Hardware- und Softwarehersteller in Deutschland oder Europa zu fördern, um eine weitgehend EU-autarke Versorgung zu gewährleisten?

    a) Welches Finanzvolumen wäre nach Meinung der Bundesregierung für eine solche Förderung notwendig?

    b) Welcher Zeitraum wäre nach Meinung der Bundesregierung für eine solche Förderung notwendig?

Nationale Fördermaßnahmen für Unternehmen sind aufgrund der auf EU-Ebene vollharmonisierten Beihilfevorschriften nicht bzw. nur sehr eingeschränkt möglich. Eine im Sinne der Fragestellung intendierte Form der Förderung könnte aber z. B. im Rahmen der von der Kommission erlassenen Mitteilung über wichtige Vorhaben von gemeinsamem europäischem Interesse (Important Projects of Common European Interest – IPCEI) erfolgen, die dazu beitragen sollen, dass vor allem große Vorhaben gefördert werden können, die das Wirtschaftswachstum, die Beschäftigung und die Wettbewerbsfähigkeit Europas spürbar erhöhen.

17. Hält die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, „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“, für realistisch und zielführend, und wird die Bundesregierung diese Forderung umsetzen?

Die Vertretung Deutschlands in den relevanten Gremien der 5G-Standardisierung erfolgt v. a. durch die Bundesnetzagentur und das Bundesamt für die Sicherheit in der Informationstechnik. Die für die 5G-Standardisierung, insbesondere im Rahmen des Third Generation Partnership Projects, vorgesehenen Haushaltsmittel werden daher als ausreichend angesehen.

18. Wie bewertet die Bundesregierung die in dem Antrag der Fraktion der AfD „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ (Bundestagsdrucksache 19/7723) aufgestellte Forderung, „bestehende 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“, und wird die Bundesregierung diese Forderung umsetzen?

Die zukünftigen 5G Netze werden auch eine Ende zu Ende Verschlüsselung auf Anwendungsebene zulassen. Die Kryptoeckpunkte der Bundesregierung haben weiterhin bestand.

19. Welche Sicherheitsrisiken sieht die Bundesregierung durch den Einsatz von Hardware- und Softwarekomponenten nichteuropäischer Hersteller auch im Bereich der Festnetzinfrastruktur, und welcher akute und strategische Handlungsbedarf folgt für die Bundesregierung aus dieser Risikobewertung?

Die Bundesnetzagentur führt ihre behördlichen Aufsichtstätigkeiten im Mobilfunk- und auch Festnetzbereich grundsätzlich hersteller- und technologieunabhängig durch. Weiterführende Erkenntnisse zu Risiken bei Beteiligung außereuropäischer Unternehmen liegen bei der Bundesnetzagentur nicht vor.

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