Deutscher Bundestag **Drucksache 20/7698**

20. Wahlperiode 11.07.2023

Kleine Anfrage

der Fraktion der CDU/CSU

Sicherheit europäischer 5G-Mobilfunknetze

Am 15. Juni 2023 wurde der Zweite Fortschrittsbericht über die Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit (EU-Toolbox on 5G Cybersecurity) veröffentlicht. Im Zuge dessen hat die Europäische Kommission eine Mitteilung zur Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit angenommen (digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox).

Darin zeigt sich die EU-Kommission „besorgt über die Risiken, die von bestimmten Mobilfunk-Netzausrüstungsanbietern für die Sicherheit der Union ausgehen“ und nennt dabei insbesondere die Anbieter Huawei und ZTE. Gleichzeitig kündigt die Kommission an, künftig zu vermeiden, dass interne Kommunikation über Mobilfunknetze, in denen Komponenten von Huawei und ZTE verbaut sind, stattfindet. Zudem sollen fortan „keine neuen Netzanbindungsdienste beschafft werden, die auf Ausrüstung dieser Anbieter angewiesen sind“.

Im Fortschrittsbericht wird dargelegt, dass bisher 21 Staaten den legislativen Rahmen geschaffen hätten, um das unterschiedliche Risikoprofil verschiedener Lieferanten zu bewerten und darauf aufbauend Restriktionen, einschließlich notwendiger Ausschlüsse, anzuwenden (digital-strategy.ec.europa.eu/de/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity). EU-Kommissar Thierry Breton kritisierte in einer Rede jedoch deutlich, dass bisher nur zehn Mitgliedstaaten tatsächlich Maßnahmen ergriffen hätten, um Hochrisikoanbieter zu beschränken oder auszuschließen. Dies sei deutlich zu langsam, stelle ein erhebliches Sicherheitsrisiko dar und kreiere wesentliche Abhängigkeiten für die EU (ec.europa.eu/commission/presscorner/detail/en/speech_23_3314).

In Deutschland wurden mit dem von der CDU/CSU-geführten Vorgängerregierung auf den Weg gebrachten IT-Sicherheitsgesetz 2.0 Instrumente geschaffen, um den Einbau von Komponenten nichtvertrauenswürdiger Hersteller in kritischen Infrastrukturen zu untersagen (§ 9b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). Zum jetzigen Zeitpunkt ist nach Kenntnis der Fragesteller jedoch keine entsprechende Untersagung erfolgt und nur erstmalig eingesetzte Komponenten wurden einer kritischen Prüfung unterzogen. Im März 2023 wurden Unternehmen der Branche in einem Schreiben darauf hingewiesen, dass künftig auch weitere kritische Komponenten überprüft werden sollen (background.tagesspiegel.de/digitalisierung/us-sanktionen-setzen-huawei-schwer-zu). Als Antwort auf die Kleine Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/6921 bestätigte die Bundesregierung, dass derzeit eine Prüfung von im Einsatz befindlichen kritischen Komponenten in 5G-Mobilfunknetzen erfolgt. Das Verfahren soll im

Sommer abgeschlossen werden (Bundestagsdrucksache 20/6921). „DER SPIEGEL“ berichtete indessen, dass das Bundesministerium des Innern und für Heimat (BMI) eine wichtige Softwarekomponente des Herstellers Huawei untersagen könnte. Dabei handle es sich um ein „Programm, mit dem die Basisstationen des chinesischen Konzerns aus der Ferne konfiguriert und gesteuert werden können“ (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71). Demnach stehen „dabei Bauteile des 4G-Netzes im Fokus, die per Software-Update 5G-fähig werden und damit kritische Funktionen für den Netzbetrieb übernehmen können. Die Befürchtung ist, dass dadurch Daten für Spionagezwecke gesammelt und im Extremfall das Handynetz manipuliert oder abgeschaltet werden könnte. Die Vorstellung, einen eindeutigen Beweis in Form eines „Kill Switches“ zu finden, halten die Sicherheitsbehörden für abwegig. Das eigentliche Risiko ergebe sich durch die Software-Updates, mit denen sich bestimmte Bauteile umprogrammieren ließen – womöglich unbemerkt von den Netzbetreibern.“ (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html).

Wir fragen daher die Bundesregierung:

1. Über welches Mobilfunknetz kommuniziert die Bundesregierung intern?
2. Wie hoch ist der Anteil von Komponenten von Huawei und ZTE in dem Mobilfunknetz, das die Bundesregierung für ihre interne Kommunikation nutzt?
3. Wie bewertet die Bundesregierung die Ankündigung der EU-Kommission, die Nutzung von Mobilfunknetzen mit Komponenten von Huawei und ZTE für die interne Kommunikation künftig zu vermeiden, und plant die Bundesregierung, der Auffassung der EU-Kommission zu folgen?
4. Plant die Bundesregierung, der EU-Kommission zu folgen, künftig keine neuen Netzanbindungsdienste zu beschaffen, die auf Ausrüstung von Huawei und ZTE angewiesen sind, wenn ja, warum, und wenn nein, warum nicht?
5. In welchen EU-Staaten gibt es nach Kenntnis der Bundesregierung chinesische Mobilfunknetzbetreiber, und stellt dies nach Auffassung der Bundesregierung ein grenzüberschreitendes Sicherheitsrisiko für die EU dar (bitte entsprechende EU-Staaten und jeweilige Mobilfunknetzbetreiber einzeln auflisten)?
6. Welche Maßnahmen hat die Bundesregierung getroffen, um gemäß den Empfehlungen der EU-Toolbox Hochrisikoanbieter (SM03) einzuschränken?
7. Sieht die Bundesregierung bei sich Versäumnisse in der Umsetzung der EU-Toolbox, insbesondere im Bereich der Anwendung von Maßnahmen zur Einschränkung von Hochrisikoanbietern, wenn ja, warum, und wenn nein, warum nicht?
8. Sind der Bundesregierung Planungen der EU-Kommission bekannt, verbindliche Vorgaben zum Ausschluss von Hochrisikoanbietern beim Ausbau von 5G-Mobilfunknetzen einführen zu wollen (www.spiegel.de/netzwelt/netzpolitik/5g-eu-erwaegt-wohl-doch-verbindliche-vorgaben-zum-huawei-ausschluss-a-5d82424a-3689-4102-a90f-8fbd268c389f), und ist die Bundesregierung in diese Planungen einbezogen?
9. Ist nach Auffassung der Bundesregierung ein EU-weites Verbot von Komponenten von Hochrisikoanbietern in 5G-Mobilfunknetzen rechtlich möglich?

10. Ist es zutreffend, dass sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der derzeit laufenden Überprüfung von Bestandskomponenten auf eine Softwarekomponente des chinesischen Herstellers Huawei konzentriert (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71)?
11. Ist es nach Kenntnis der Bundesregierung technisch zutreffend, dass in Basisstationen deutscher Mobilfunknetze Softwarekomponenten verbaut sind, die aus China konfiguriert und gesteuert werden können (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71)?
12. Was genau könnte nach Kenntnis der Bundesregierung mit den in Rede stehenden Softwarekomponenten aus China heraus konfiguriert und gesteuert werden?
13. Ist es nach Kenntnis der Bundesregierung zutreffend, dass im Extremfall das Mobilfunknetz aus China heraus abgeschaltet werden könnte (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html)?
14. Hält die Bundesregierung es für möglich, dass Software-Updates bei Mobilfunk-Komponenten mit Fernwartungsfunktionen vollständig überprüft und ihre Sicherheit garantiert werden können (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html)?
15. Teilt die Bundesregierung, die Auffassung des Bundesministers für Wirtschaft und Klimaschutz Dr. Robert Habeck, derzufolge „Deutschland […] künftig keine Huawei-Produkte mehr in modernen 5G-Mobilfunknetzen verbauen [will].“ (www.spiegel.de/netzwelt/netzpolitik/5g-eu-erwaegt-wohl-doch-verbindliche-vorgaben-zum-huawei-ausschluss-a-5d82424a-3689-4102-a90f-8fbd268c389f)?
16. Wie viel Prozent der in Deutschland ansässigen Unternehmen sind von Mobilfunknetzen mit verbauten Komponenten chinesischer Hersteller abhängig?
17. Welche weiteren Bundesbehörden sind neben dem BSI an der derzeit laufenden Prüfung der kritischen Komponenten im Mobilfunknetz beteiligt (bitte auflisten)?
18. Welche weiteren Bundesministerien wurden von Beginn an vom BMI mit in den in Frage 17 genannten Prüfungsprozess einbezogen?
19. Werden seitens der Bundesregierung auch Sicherheitsbehörden der Länder an der Prüfung beteiligt?
20. Wird seitens der Bundesregierung auch die Bundeswehr (Kommando Cyber- und Informationsraum, Kommando CIR) an der Prüfung beteiligt?
21. Würde das Kommando CIR im Spannungsfall (Artikel 80a des Grundgesetzes – GG) federführend die Aufgabe des Cyberschutzes der kritischen Infrastrukturen übertragen bekommen, wenn ja, für welche kritischen Infrastrukturen wäre das Kommando CIR im Spannungsfall federführend zuständig (bitte auflisten), und wenn nein, bleiben auch im Spannungsfall die Betreiber für den Cyberschutz der kritischen Infrastrukturen zuständig?

    Welche Rolle nimmt das BSI im Spannungsfall beim Cyberschutz kritischer Infrastrukturen ein?

22. Würde das Kommando CIR im Verteidigungsfall (Artikel 115a GG) federführend die Aufgabe des Cyberschutzes der kritischen Infrastrukturen übertragen bekommen, wenn ja, für welche kritischen Infrastrukturen wäre das Kommando CIR im Verteidigungsfall federführend zuständig (bitte auflisten), und wenn nein, bleiben auch im Verteidigungsfall die Betreiber für den Cyberschutz der kritischen Infrastrukturen zuständig?

    Welche Rolle nimmt das BSI im Verteidigungsfall beim Cyberschutz kritischer Infrastrukturen ein?

23. Führt die Bundesregierung Übungen durch, in denen das Zusammenspiel von Kommando CIR und weiteren Sicherheitsbehörden zum Cyberschutz kritischer Infrastrukturen im Spannungs- oder Verteidigungsfall geübt wird?

24. Verbaut die Deutsche Bahn nach Kenntnis der Bundesregierung weiterhin Komponenten von Huawei „zum Aufbau eines betriebsinternen IT-Netzwerks“ (www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-ampel-politiker-fordern-ausschluss-von-huawei-bei-der-deutschen-bahn/29081420.html), und wie bewertet die Bundesregierung diesen Sachverhalt?

25. Teilt die Bundesregierung die Auffassung der Deutschen Bahn AG, der zufolge für „Netzwerk-Infrastruktur keine Meldepflicht bestehe, weil das Funknetz der DB Netz nicht öffentlich sei. Das Bundesamt für Sicherheit in der Informationstechnik betonte, dass die IT-Systeme der Bahn bislang nicht als kritisch eingestuft würden“ (www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-ampel-politiker-fordern-ausschluss-von-huawei-bei-der-deutschen-bahn/29081420.html), und wenn ja, bitte begründen?

26. In welchen weiteren internen IT-Systemen und Mobilfunknetzen verbaut die Deutsche Bahn AG derzeit nach Kenntnis der Bundesregierung Komponenten chinesischer Hersteller?

27. Bezugnehmend auf die Antwort zu Frage 17 auf Bundestagsdrucksache 20/6271 – hat die Bundesregierung inzwischen überprüft, ob die Bundeswehr Komponenten chinesischer Hersteller gekauft oder in Anwendung hat?

28. Bezugnehmend auf die Antwort zu Frage 17 auf Bundestagsdrucksache 20/6271 – in Bezug auf welche Bereiche der Bundeswehr und in Bezug auf welche Produkte hat die Bundesregierung den Verdacht, dass die Bundeswehr Komponenten chinesischer Hersteller gekauft oder in Anwendung hat?

29. Bezugnehmend auf die Antwort zu Frage 25 auf Bundestagsdrucksache 20/6271, der zufolge „die Bundesregierung Kenntnis über verwendete kritische Komponenten im Sinne des § 2 Absatz 13 BSIG aufgrund der beim BMI nach § 9b Absatz 1 BSIG eingehenden Anzeigen“ erlangt – wie hoch ist der Anteil an kritischen Komponenten chinesischer Hersteller in den deutschen Mobilfunknetzen?

30. Bezugnehmend auf die Antwort zu Frage 2 auf Bundestagsdrucksache 20/6921), der zufolge das BMI die „Betreiber von öffentlichen 5G-Mobilfunknetzen am 6. März 2023 aufgefordert [hat], alle in den jeweiligen Netzen im Einsatz befindlichen kritischen Komponenten der Hersteller Huawei und ZTE mitzuteilen und nach einer vorgegebenen Systematik aufzulisten.“ – haben inzwischen alle Betreiber von öffentlichen 5G-Mobilfunknetzen dem BMI geantwortet und ihre kritischen Komponenten der Hersteller Huawei und ZTE mitgeteilt und diese nach der vorgegebenen Systematik aufgelistet, und wenn nein, welche Betreiber von öffentlichen 5G-Mobilfunknetzen haben nicht oder nicht vollständig geantwortet?

31. Kann die Bundesregierung den im Presseartikel genannten Anteil an chinesischen Komponenten im deutschen Mobilfunknetz bestätigen „Andere Länder in Europa haben längst gehandelt und chinesische Komponenten komplett aus ihren Netzen verbannt. Darunter: Estland, Lettland, Litauen, Norwegen, Schweden, Dänemark, Tschechien, die Slowakei und Luxemburg. Frankreich hat den Anteil von 26 auf 17 Prozent gesenkt. In Deutschland aber ist der Anteil chinesischer Technik in den Mobilfunknetzen gestiegen: Von 57 auf 59 Prozent.“ (www.zdf.de/nachrichten/politik/mobilfunknetz-ausbau-technik-china-sicherheitsrisiko-100.html)?

32. Wenn der Bundesregierung gemäß Antwort zu Frage 2d auf Bundestagsdrucksache 20/6921 „Anhaltspunkte für eine mögliche voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit der Bundesrepublik Deutschland durch Komponenten der Hersteller Huawei und ZTE, die als kritische Komponenten in öffentlichen 5G-Mobilfunknetzen eingesetzt werden, vor[liegen]“ – wann beabsichtigt die Bundesregierung, darauf zu reagieren?

33. Aus welchen Gründen ist nach Kenntnis der Bundesregierung in der Kategorie „Radio Access Network“ (RAN) der „Liste der kritischen Funktionen“ nach § 109 Absatz 6 Satz 1 Nummer 2 TKG [Telekommunikationsgesetz] für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ (www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf?__blob=publicationFile&v=3) lediglich das 5G-RAN-Management als kritische Funktionalität gemäß § 109 Absatz 6 Satz 1 Nummer 2 TKG eingestuft?

34. Welche weiteren Funktionalitäten werden nach Kenntnis der Bundesregierung durch das RAN erfüllt, und warum werden diese nicht als kritische Funktionen eingestuft?

35. Warum wird nach Kenntnis der Bundesregierung insbesondere das eNodeB-Netzelement nicht als kritische Funktion gemäß § 109 Absatz 6 Satz 1 Nummer 2 TKG in der Kategorie „Radio Access Network“ der „Liste der kritischen Funktionen nach § 109 Absatz 6 Satz 1 Nummer 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ (www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.html) eingestuft?

36. Wie oft haben Betreiber kritischer Infrastrukturen seit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 im Mai 2021 den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 BSI-Gesetz dem Bundesministerium des Innern und für Heimat angezeigt (bitte für 2021, 2022 und das erste Halbjahr 2023 separat auflisten)?

Wie oft wurde der Einsatz der kritischen Komponenten gemäß § 9b BSI-Gesetz untersagt, und wie oft waren Komponenten chinesischer Hersteller betroffen (bitte für 2021, 2022 und das erste Halbjahr 2023 separat auflisten)?

Berlin, den 10. Juli 2023

Friedrich Merz, Alexander Dobrindt und Fraktion

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