1582/J
vom 22.04.2020 (XXVII. GP)

Anfrage

der Abgeordneten Mag.[a] Dr.[in] Petra Oberrauner, Genossinnen und Genossen

an den Bundeskanzler

betreffend Sicherheitsbedenken beim 5G-Ausbau

Mit dem Aufbau des 5G-Netzwerkes in Österreich wird eine fundamentale Intensivierung der gesellschaftlichen und wirtschaftlichen Digitalisierung eingeleitet. 5G wird die mobile Datenübertragung schneller, intelligenter und modularer machen und damit die digitale Vernetzung in allen Lebensbereichen vorantreiben. Das Internet der Dinge (die Kommunikation von Produktionsmaschinen und smarten Gebrauchsgegenständen untereinander) wird genauso über 5G stattfinden, wie wirtschaftliche Geschäftsprozesse, die digitale Kommunikation in Universitäten und Krankenhäusern und die Steuerung von Infrastruktur (z.B. Verkehr, Stromerzeugung und Stromnetze). Damit wird die digitale Infrastruktur (sowohl festnetz- wie funkbasiert) zwangsläufig zum Bestandteil der kritischen Infrastruktur Österreichs. Wenn es um den Aufbau, den Ausbau und die Instandhaltung des 5G-Netzwerkes geht, müssen daher höchste Sicherheitsanforderungen gelten.
Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE

1. Gab es in den vergangenen drei Jahren Gespräche zwischen ihrem Ressort und Netzwerkausrüstern im Bereich von 5G und wenn ja, um welche Unternehmen handelt es sich und wie viele Gespräche haben stattgefunden?

2. Welche europäischen, amerikanischen und chinesischen Unternehmen sind nach ihrer Sicht in der Lage, Komponenten für den Ausbau des österreichischen 5G-Netzes bereitzustellen (darunter sind Unternehmen zu verstehen, die spezialisierte Lösungen für die Kern- und Zugangsnetze der in Österreich tätigen Mobilfunknetzbetreiber liefern)?

3. Gibt es österreichische Unternehmen, die Komponenten zum Aufbau der 5GTechnologie bereitstellen könnten?

4. Was halten Sie von sogenannten No-Spy-Klauseln und sollen diese beim 5G-Ausbau zur Anwendung kommen?

5. Wie schätzen Sie die Risiken der Verwendung von Netzwerktechnik von Anbietern aus Nicht-EU-Ländern für Spionageaktivitäten und gezielte Netzstörungen ein, und worauf stützen Sie ihre Einschätzung?

6. Mit welchen Maßnahmen wollen Sie das Risiko von Spionageaktivitäten und Netzstörungen mit Hilfe der Netzwerktechnik verhindern?

7. Welche weiteren Risiken sehen Sie bei Beteiligungen von Unternehmen aus Nicht-EU-Ländern sowie Unternehmen aus undemokratischen Staaten an sensibler Infrastruktur? Unterscheiden Sie bei diesen Risiken zwischen Kernnetz und Zugangsnetz?

8. Führen Sie einen Sicherheitskatalog für den Aufbau sensibler Infrastrukturprojekte wie dem 5G-Netz? Falls ja, welche Kriterien werden in diesem Katalog gelistet? Falls nein, warum nicht und ist so ein Katalog geplant?

9. Für wie hoch halten Sie das Risiko, dass Netzwerkausrüster aus Nicht-EU-Ländern Backdoors in ihren Source-Code programmieren, um ihren Heimatstaaten Zugriff auf das österreichische 5G-Netz zu verschaffen?

10. Ist es ihrer Ansicht nach möglich, wöchentliche Software Updates der Netzwerkausrüster vorab zu kontrollieren, um sicherzugehen, dass keine Spionage- oder Sabotagesoftware eingeschleust wird? Falls nein, wie soll die Sicherheit des österreichischen Netzwerks sichergestellt werden?

11. Wie werden Sie sicherstellen, dass die Regierungen der Heimatländer der beteiligten Netzwerkhersteller nicht mit Hilfe gesetzlicher oder technischer Mittel auf Daten der von diesen Unternehmen produzierten und in Österreich eingesetzten Telekommunikationsprodukte zugreifen können?

12. Haben Sie eine Risikoanalyse für das zukünftige österreichische 5G-Netzwerk durchgeführt?

13. Was waren die Hauptbedrohungsszenarien, die sie berücksichtigt haben?

14. Von welchen Bedrohungen und Bedrohungsakteuren gehen sie mit Blick auf die österreichischen 5G-Netzwerke aus (Aufzählung bitte jeweils nach Gewichtung)?

15. Inwiefern berücksichtigen Sie aus Sicherheitsgründen die Vertrauenswürdigkeit des Herstellers und seines Heimatlandes in den Bereichen Demokratie, Datenschutz, Rechtstaatlichkeit und Menschenrechte als Kriterium für die Beteiligung am Aufbau kritischer digitaler Infrastrukturen wie 5G?

16. Inwiefern berücksichtigen Sie sicherheitsstrategische und wirtschaftsstrategische Überlegungen als Kriterien für die Beteiligung am Aufbau kritischer digitaler Infrastrukturen wie 5G?

17. Inwiefern berücksichtigen Sie die Gefahren einer wachsende Abhängigkeiten von Herstellern und deren Herkunftsländern im Bereich kritischer digitaler Infrastrukturen, etwa wenn notwendige Software-Updates für diese Infrastrukturen verweigert werden können?

18. Gibt es mit Bezug auf den 5G-Netzausbau eine Koordinierung im Bereich der damit verbundenen Cybersecurity zwischen Österreich der Europäischen Kommission und den übrigen EU-Mitgliedsländern? Falls ja, wie sieht diese Koordinierung konkret aus? Falls nein, warum nicht?

19. Wie stellen Sie sicher, dass die 3- und 4G-Netzwerke in Österreich sicher sind?

20. Welche privaten oder staatlichen Unternehmen aus Nicht-EU-Staaten sowie EU-Unternehmen die mehrheitlich Konzernen aus Nicht-EU-Staaten gehören, sind Lieferanten/ Zulieferer für die derzeit verwendete digitale Infrastruktur der Bundesregierung, der Ministerien und der Bundesbehörden?

21. Um welche Produkte handelt es sich dabei?

22. Wie hoch ist die Abhängigkeit von Netzwerkherstellern aus Nicht-EU-Ländern bei der Errichtung und Instandhaltung der 3-,4- und 5G-Netzwerke?

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-04-22T12:16:37+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	