bmi.gv.at

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.136.256

Wien, am 19. März 2020

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Mag.[a] Dr.[in] Petra Oberrauner, Genossinnen und Genossen haben am 22. Jänner 2020 unter der Nr. **634/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Sicherheitsbedenken beim 5G-Ausbau“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zur Frage 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?*

Den Staatsschutzbehörden obliegt zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit, die Förderung der Bereitschaft und Fähigkeit des Einzelnen, sich über eine Bedrohung seiner Rechtsgüter Kenntnis zu verschaffen und Angriffen entsprechend vorzubeugen. Im Rahmen dieser gesetzlichen Aufgabe werden auch Sensibilisierungsgespräche, insbesondere mit Betreibern kritischer Infrastrukturen, geführt.

Von den Staatsschutzbehörden wurden keine bilateralen Gespräche mit Netzwerk-ausrüstern im Bereich von 5G geführt. Es besteht jedoch ein reger Informationsaustausch

im Rahmen von Cyber-Planspielen, an denen Vertreter anderer Bundesministerien, Stakeholder aus der Wirtschaft sowie das Cyber Security Center im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung teilnehmen.

Zu den Fragen 2, 4, 5, 9, 10, 16 bis 19 und 27:

- *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)?*
- *Was halten Sie von sogenannten No-Spy-Klauseln und sollen diese beim 5G-Ausbau zur Anwendung kommen?*
- *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?*
- *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?*
- *1Ist es ihrer Ansicht nach möglich, wöchentliche Software Updates der Netzwerk-ausrüster vorab zu kontrollieren, um sicherzugehen, dass keine Spionage- oder Sabotagesoftware eingeschleust wird? Falls nein, wie soll die Sicherheit des österreichischen Netzwerks sichergestellt werden?*
- *Wie bewerten Sie die Vertrauenswürdigkeit des Herstellers und seines Heimatlandes in den Bereichen Demokratie, Datenschutz, Rechtstaatlichkeit und Menschenrechte als Kriterium für die Beteiligung kritischer digitaler Infrastrukturen wie 5G?*
- *Wie bewerten Sie sicherheitsstrategische und wirtschaftsstrategische Überlegungen als Kriterium für die Beteiligung kritischer digitaler Infrastrukturen wie 5G?*
- *Wie bewerten Sie die Gefahren durchwachsende Abhängigkeiten von Herstellern und ihren Herkunftsländern, etwa wenn notwendige Software-Updates verweigert werden BMVIT können?*
- *Wie bewerten Sie die Beauftragung österreichischer und EU-Unternehmen vor dem Hintergrund des Ziels die österreichische und EU-Wirtschaft in diesem Bereich wettbewerbsfähig zu halten?*
- *Für wie hoch schätzen Sie die Abhängigkeit von Netzwerkherstellern aus Nicht-EU-Ländern bei der Errichtung und Instandhaltung der 3-,4- und 5G-Netzwerke ein?*

Dem parlamentarischen Interpellationsrecht unterliegen nur Handlungen und Unterlassungen. Da diese Fragen keinen Gegenstand der Vollziehung des Bundesministeriums

für Inneres betreffen, sondern Meinungen und Einschätzungen einfordern, sind sie somit keiner Beantwortung durch den Bundesminister für Inneres zugänglich.

Zu den Fragen 3, 7, 8, 11, 15 und 20 bis 26:

- *Gibt es österreichische Unternehmen, die Komponenten zum Aufbau der 5G-Technologie bereitstellen könnten?*
- *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?*
- *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?*
- *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?*
- *Wer entscheidet in Österreich darüber, wer am Aufbau des 5G-Netzes beteiligt werden darf und welche Kriterien sind für die Beteiligung ausschlaggebend (Auflistung bitte nach Gewichtung)?*
- *Gibt es beim 5G-Netzausbau eine Koordinierung zwischen Österreich der Europäischen Kommission und den übrigen EU-Mitgliedsländern? Falls ja, wie sieht diese Koordinierung konkret aus? Falls nein, warum nicht?*
- *Gibt es eine gemeinsame 5G-Strategie in der EU oder zumindest Leitfäden für die Mitgliedsländer?*
- *Falls es Leitfäden gibt - wo folgen Sie diesen Leitfäden und wo nicht und aus welchen Gründen?*
- *Welche Netzwerkhersteller sind mit welchen Marktanteilen an den österreichischen 3- und 4G Netzwerken beteiligt?*
- *Wie stellen Sie sicher, dass die 3- und 4G-Netzwerke in Österreich sicher sind?*
- *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?*
- *Um welche Produkte handelt es sich dabei?*

Diese Fragen fallen nicht in die Ingerenz des Bundesministers für Inneres und stellen daher keinen Gegenstand der Vollziehung des Bundesministeriums für Inneres dar, weswegen

dazu auch nicht im Wege einer parlamentarischen Anfrage durch den Bundesminister für Inneres inhaltlich Stellung genommen werden kann.

Zur Frage 6:

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

Eine vollkommene Verhinderung von Spionageaktivitäten und Netzstörungen mit Hilfe der Netzwerktechnik ist aufgrund der Komplexität des Cyberbereichs nicht möglich. Das Bundesministerium für Inneres setzt bereits jetzt – vor allem im präventiven Bereich – Maßnahmen, um die Cybersicherheit zu erhöhen.

Im Regierungsprogram 2020 sind Maßnahmen definiert, deren Ziel die weitere Stärkung der Cybersicherheit ist. Hierzu zählen vor allem die Schaffung eines staatlichen Cybersicherheitszentrums, die Stärkung der Zusammenarbeit mit Wissenschaft und Forschung oder auch Aus- und Fortbildungsmaßnahmen für IT-Spezialistinnen und -Spezialisten zur Schaffung von „Cyber Cops“ im Bundesministerium für Inneres.

Zu den Fragen 12 bis 14:

- *Haben Sie eine Risikoanalyse für das zukünftige österreichische 5G-Netzwerk durchgeführt?*
- *Was waren die Hauptbedrohungsszenarien, die sie berücksichtigt haben?*
- *Von welchen Bedrohungen und Bedrohungsakteuren gehen sie mit Blick auf die österreichischen 5G-Netzwerke aus (Aufzählung bitte jeweils nach Gewichtung)?*

Eine Risikoanalyse wurde von der RTR-GmbH in einer Zusammenarbeit von Experten der Sicherheitsressorts – darunter auch Experten des Bundesministeriums für Inneres - und der Telekommunikations- und Internetbranche aufgesetzt und konnte im Juni 2019 erfolgreich abgeschlossen werden. Damit konnte das Bundeskanzleramt die Ergebnisse der österreichischen Analyse fristgerecht an die Europäische Kommission übermitteln.

Auf europäischer Ebene wurden die Ergebnisse der nationalen 5G-Cybersicherheitsanalysen der Mitgliedsstaaten aggregiert und ein unionsweites Lagebild erstellt. Die Ergebnisse wurden in einem Bericht zusammengefasst, welcher am 9. Oktober 2019

veröffentlicht wurde. Dieser Bericht ist unter https://www.rtr.at/de/tk/5GCybersicherheitsanalyse2019 abrufbar.

Die konkreten Inhalte der österreichischen Analyse können aufgrund der Verpflichtung zur Amtsverschwiegenheit gemäß Art. 20 Abs. 3 B-VG nicht preisgegeben werden.

Karl Nehammer, MSc

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2020-03-20T08:55:10+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1710479
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-03-20T09:01:05+01:00
	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.	