

**Elisabeth Köstinger**  
Bundesministerin für  
Landwirtschaft, Regionen und Tourismus

Herrn  
Mag. Wolfgang Sobotka  
Präsident des Nationalrats  
Parlament  
1017 Wien

Geschäftszahl: 2020-0.071.278

Ihr Zeichen: BKA – PDion (PDion)633/J-NR/2020

Wien, 20.03.2020

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Mag.<sup>a</sup> Dr.<sup>in</sup> Petra Oberrauner, Kolleginnen und Kollegen haben am 22.01.2020 unter der Nr. **633/J** an die Bundesministerin für Verkehr, Innovation und Technologie eine schriftliche parlamentarische Anfrage betreffend „Sicherheitsbedenken beim 5G-Ausbau“ gerichtet.

Mit Inkrafttreten der BMG-Novelle 2020, BGBl. I, Nr. 8/2020 am 29. Jänner 2020 kam es zu Änderungen der Zuständigkeiten der Bundesministerien, woraufhin die Anfrage an das nunmehr zuständige Bundesministerium für Landwirtschaft, Regionen und Tourismus weitergeleitet wurde.

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?

Seitens des Ressorts ist eine Bereitschaft gegeben, mit allen am Markt tätigen Stakeholdern zu sprechen, diese Kontakte finden laufend in unterschiedlichstem Rahmen statt. Mit Vertretern des Ausrüsters Huawei beispielsweise haben zwei Gespräche stattgefunden.

Bis zum Inkrafttreten der BMG-Novelle 2020, BGBl. I, Nr. 8/2020 am 29. Jänner 2020 lag die diesbezügliche Zuständigkeit im vormaligen Bundesministerium für Verkehr, Innovation und Technologie.

**Zu den Fragen 2, 3 und 15:**

- 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)?
- Gibt es österreichische Unternehmen, die Komponenten zum Aufbau der 5G-Technologie bereitstellen könnten?
- 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)?

Für den Netz-Roll-Out sind die Telekom-Unternehmen zuständig, weshalb diesen auch die Auswahl der Netzwerkhersteller obliegt. Es gelten die gesetzlichen Regelungen des Telekommunikationsgesetzes und der einschlägigen Verordnungen.

Seitens des Bundesministeriums für Landwirtschaft, Regionen und Tourismus wird keine Beurteilung dazu vorgenommen, welche Unternehmen in der Lage sind, Komponenten für den Ausbau der österreichischen 5G-Netze zu liefern.

**Zur Frage 4:**

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

Das Bundesministerium für Landwirtschaft, Regionen und Tourismus ist in die Vertragsgestaltung zwischen Netzbetreibern und Netzwerkherstellern nicht eingebunden. Die Regulierungsbehörde erarbeitet derzeit den Entwurf einer Netzsicherheitsverordnung. Diese Verordnung wird verschiedene Maßnahmen zur Sicherstellung der Netzsicherheit vorsehen, welche von den Unternehmen auch in den Verträgen abzubilden sein werden.

**Zu den Fragen 5 bis 11 und 24:**

- 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?
- Mit welchen Maßnahmen wollen Sie das Risiko von Spionageaktivitäten und Netzstörungen mit Hilfe der Netzwerktechnik verhindern?
- 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?
- 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?
- 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?
- 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?
- Wie stellen Sie sicher, dass die 3- und 4G-Netzwerke in Österreich sicher sind?

Die Angelegenheiten der Cybersicherheit fallen in den Zuständigkeitsbereich des Bundeskanzleramtes. Eine derartige Einschätzung kann daher vom Bundesministerium für Landwirtschaft, Regionen und Tourismus nicht vorgenommen werden.

Einzigster Anknüpfungspunkt sofern Telekommunikationsnetze betroffen sind, sind rechtliche Festlegungen in der Netzsicherheitsverordnung, welche detaillierte Vorgaben für Netzbetreiber betreffend die Sicherheit und Integrität von Netzen enthalten wird. Diese Verordnung wird derzeit – unter anderem als Folge der laufenden Diskussionen zur Sicherheit von 5G-Netzen – erarbeitet. Zuständig ist die Rundfunk und Telekom Regulierungs-GmbH.

Die Sicherheit für die 3G- und 4G-Netzwerke in Österreich wird durch das Telekommunikationsgesetz sowie zukünftig auch durch die Netzsicherheitsverordnung und deren Vollzug gewährleistet. Diese Bestimmungen sind für alle Diensteanbieter unabhängig von der angewandten Technologie verbindlich.

**Zu den Fragen 12 bis 14, 18 und 20:**

- 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)?
- Wie bewerten Sie die Gefahren durch wachsende Abhängigkeiten von Herstellern und ihren Herkunftsländern, etwa wenn notwendige Software-Updates verweigert werden können?
- 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?

In Sachen Sicherheit kritischer Infrastrukturen wie 5G besteht der gewählte Ansatz darin, ein gemeinsames europäisches Vorgehen festzulegen.

Der Europäische Rat rief die Mitgliedstaaten auf, nationale Risikobewertungen durchzuführen und staatliche Maßnahmen zu überprüfen sowie auf Ebene der Europäischen Union zusammenzuarbeiten, um eine koordinierte Risikobewertung und ein Instrumentarium möglicher Maßnahmen zur Risikominderung zu erarbeiten.

Basierend auf diesen Risikobewertungen veröffentlichte die „NIS (Netz- und Informationssysteme) Cooperation Group“ auf Ebene der Europäischen Union einen Bericht über die EU-weit koordinierte Risikobewertung zur Cybersicherheit in 5G-Netzen. Dieser umfasst die Hauptbedrohungen und deren Verursacher, die anfälligsten Anlagen und Einrichtungen sowie die wichtigsten Schwachstellen (technischer und anderer Art), von denen 5G-Netze betroffen sind und listet Risikokategorien zu fünf verschiedenen Risikovarianten auf:

| Risikoszenarien   | Risikokategorien   |
|---|--|
| Risikoszenarien im Zusammenhang mit unzureichenden Sicherheitsmaßnahmen | <b>R1:</b> Fehlkonfiguration von Netzen  |
|   | <b>R2:</b> Mangelnde Zugangskontrolle  |
| Risikoszenarien im Zusammenhang mit der 5G-Lieferkette                  | <b>R3:</b> Schlechte Produktqualität   |
|   | <b>R4:</b> Abhängigkeit von einem einzelnen Anbieter innerhalb einzelner Netze oder mangelnde landesweite Vielfalt |

|   |   |
|---|---|
| Risikoszenarien im Zusammenhang mit der Vorgehensweise der wichtigsten Bedrohungsakteure                            | <b>R5:</b> Staatliche Einflussnahme über die 5G-Lieferkette   |
|   | <b>R6:</b> Nutzung von 5G-Netzen durch organisierte Kriminalität oder Verbrechergruppen, die es auf Endnutzer abgesehen haben |
| Risikoszenarien im Zusammenhang mit gegenseitigen Abhängigkeiten zwischen 5G-Netzen und anderen kritischen Systemen | <b>R7:</b> Erhebliche Störung kritischer Infrastrukturen oder Dienste   |
|   | <b>R8:</b> Massive Netzausfälle aufgrund einer Unterbrechung der Stromversorgung oder Störungen anderer Unterstützungssysteme |
| Risikoszenarien im Zusammenhang mit Geräten der Endnutzer   | <b>R9:</b> Ausnutzung des Internets der Dinge (IoT)   |

Die Bewertung der Risiken R1 bis R9 erfolgte hinsichtlich:

- Eintrittswahrscheinlichkeit
- Umsetzungsfaktor (Kosten, wirtschaftliche Auswirkungen, ...)
- Umsetzungszeitraum (bis zur Wirksamkeit der Maßnahme)

Der Bericht enthält auch Aspekte bzw. Herausforderungen die im Zusammenhang mit 5G-Netzen von Bedeutung sind:

- Durch die, durch 5G-Technologie eingeleiteten technischen Veränderungen werden die Gesamtangriffsfläche und die Zahl der möglichen Angriffspunkte erhöht.
- Durch die neuen technischen Merkmale gewinnt die Abhängigkeit der Mobilfunknetzbetreiber von Drittanbietern und deren Rolle in der 5G-Lieferkette an Bedeutung. Dadurch erhöht sich nicht nur die Zahl der potentiellen Angriffswege, die von Angreifern – insbesondere von Akteuren, die von Nicht-EU-Staaten geführt oder unterstützt werden – gewählt werden könnten, sondern auch die mögliche Schwere der Auswirkungen solcher Angriffe.
- Eine hohe Abhängigkeit von einem einzigen Anbieter steigert die Gefahr und die Folgen eines möglichen Ausfalls dieses Anbieters. Dadurch verschärfen sich auch die potenziellen Folgen von Schwachstellen und Anfälligkeiten und deren möglicher Ausnutzung durch Angreifer, insbesondere bei einer Abhängigkeit von einem Anbieter, der ein hohes Risiko aufweist.

Basierend auf den einzelnen mitgliedstaatlichen Risikobewertungen hat die „NIS Cooperation Group“ im Jänner 2020 eine „EU-Toolbox für Maßnahmen der Risikominimierung“ veröffentlicht. Diese unterteilt die vorgeschlagenen Risikominimierungsinstrumente in drei Bereiche, die auf nationaler Ebene einfließen sollen:

1. Strategische Maßnahmen:
  - Stärkung von regulatorischen/hoheitlichen Befugnissen
  - Bewertung der Risikoprofile von Lieferanten und Drittanbietern
  - Diversifizierung von Lieferanten
  - Nachhaltigkeit und Vielfalt der 5G Liefer- und Wertschöpfungskette
2. Technische Maßnahmen:
  - Netzwerksicherheit – Basismaßnahmen
  - Netzwerksicherheit – 5G Spezifische Maßnahmen
  - Anforderungen an die Lieferantenprozesse und -ausrüstung
  - Belastbarkeit und Kontinuität
3. Unterstützende Maßnahmen:
  - Netzwerksicherheit
  - Standardisierung
  - Drittanbieter
  - Belastbarkeit und Kontinuität
  - Kooperation und Koordination
  - Öffentliche Beschaffung

Seitens der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) wird auf Basis der Ergebnisse der Risikobewertung ein Vorschlag für eine Verordnung, die einerseits Aspekte der Netzinformationssicherheit (NIS) und andererseits Spezialthemen der 5G-Sicherheit (5G-Toolbox der Europäischen Union) regeln soll, erarbeitet.

**Zur Frage 15:**

- 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)?

Für den Netz-Roll-Out sind die Telekom-Unternehmen zuständig, somit obliegt diesen auch die Auswahl der Netzwerkhersteller. Es gelten die gesetzlichen Regelungen des Telekommunikationsgesetzes und der einschlägigen Verordnungen, insbesondere die bei der Rundfunk und Telekom Regulierungs-GmbH in Vorbereitung befindliche Netzsicherheitsverordnung.

**Zu den Fragen 16, 17, 19, 25 und 26:**

- Wie bewerten Sie die Vertrauenswürdigkeit des Herstellers und seines Heimatlandes in den Bereichen Demokratie, Datenschutz, Rechtsstaatlichkeit 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 Beauftragung österreichischer und EU-Unternehmen vor dem Hintergrund des Ziels die österreichische und EU-Wirtschaft in diesem Bereich wettbewerbsfähig zu halten?
- 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 betreffen keinen Gegenstand der Vollziehung des Bundesministeriums für Landwirtschaft, Regionen und Tourismus.

**Zu den Fragen 21 und 22:**

- 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?

Hierzu gibt es eine Mitteilung der Europäischen Kommission vom 14. September 2016 „5G für Europa: ein Aktionsplan“ (COM/2016/0588 final) mit der eine europäische Spitzenposition in Sachen 5G-Ausbau gesichert werden soll.

Die derzeit laufende Sicherheitsdiskussion war damals noch nicht Gegenstand von Überlegungen. Diese Diskussion wurde jedoch im Rahmen der Arbeiten zur Toolbox geführt. Es wird auf die Beantwortung der Fragen 12 bis 14, 18 und 20 verwiesen.

**Zu den Fragen 23 und 27:**

- Welche Netzwerkhersteller sind mit welchen Marktanteilen an den österreichischen 3- und 4G Netzwerken beteiligt?
- 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 Bundesministerium für Landwirtschaft, Regionen und Tourismus liegen keine diesbezüglichen Daten vor.

Elisabeth Köstinger





