981/AB
vom 17.04.2020 zu 954/J (XXVII. GP)

bmi.gv.at

Bundesministerium
Inneres

Karl Nehammer, MSc
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.187.417

Wien, am 17. April 2020

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Dr. Helmut Brandstätter, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen haben am 19. Februar 2020 unter der Nr. **954/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Crypto und 5G“ gerichtet.

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

Zur Frage 1:

- *Welche Rolle spielen die Enthüllungen der Washington Post in den Überlegungen der Bundesregierung in Hinblick auf Entscheidungen, 5G-Equipment von chinesischen Unternehmen wie Huawei oder ZTE zu beziehen, bzw. solche Unternehmen in Österreich auszuschließen?*

Die Beantwortung von Fragen nach der Überlegung der Bundesregierung fällt nicht in den Vollzugsbereich des Bundesministers für Inneres,, weswegen dazu nicht im Wege einer parlamentarischen Anfrage durch das Bundesministerium für Inneres inhaltlich Stellung genommen werden kann.

Auf die Beantwortung der Anfrage 953/J XXVII. GP an das Bundesministerium für Landwirtschaft Regionen und Tourismus vom 19. Februar 2020 wird verwiesen.

Zur Frage 2:

- *Über welche Schutzvorrichtungen verfügt Österreich, um den Einbau potenzieller Backdoors, die Cyberspionage ermöglichen, durch einen privaten Anbieter, wie zum Beispiel Huawei oder ähnliche chinesische Unternehmen, zu verhindern oder zu erkennen?*

Die Frage betrifft keinen Gegenstand der Vollziehung des Bundesministeriums für Inneres und entzieht sich somit einer Beantwortung durch den Bundesminister für Inneres. Es darf aber auf die Beantwortung der korrespondierenden Anfrage 955/J XXVII. GP der Abgeordneten Dr. Helmut Brandstätter und Douglas Hoyos-Trauttmansdorff vom 19. Februar 2020 durch den Bundeskanzler verwiesen wird.

Zu den Fragen 3 und 4:

- *Gibt es im Ministerium oder anderswo im staatlichen Sicherheitsapparat eine interne Kapazität, Hardware wie jene, die Huawei oder ähnliche chinesische Unternehmen für den 5G-Ausbau zur Verfügung stellen würden, zu testen?*
  a. *Wenn ja, wo?*
  b. *Wenn nein, wie wird die Sicherheit der Hardware sonst gewährleistet?*
- *Gibt es im Ministerium oder anderswo im staatlichen Sicherheitsapparat eine interne Kapazität, Software wie jene, die Huawei oder ähnliche chinesische Unternehmen für den 5G-Ausbau zur Verfügung stellen würden, zu testen?*
  a. *Wenn ja, wo?*
  b. *Wenn nein, wie wird die Sicherheit der Software sonst gewährleistet?*

Derartige fachliche Kapazitäten bestehen im Bundesministerium für Inneres nicht. Es fällt aber auch nicht in den Aufgabenbereich des Bundesministeriums für Inneres Hard- und Softwaretests durchzuführen. Im Übrigen darf auf die Beantwortung der korrespondierenden Anfrage 952/J XXVII. GP durch die zuständige Bundesministerin für Digitalisierung und Wirtschaftsstandort verwiesen werden.

Zur Frage 5:

- *Hat das Ministerium Kenntnis darüber, ob es bereits bei 3G- und 4G-Equipment von Huawei und ähnlichen chinesischen Unternehmen Verdachtsfälle von Cyberspionage oder ähnlichen Sicherheitsrisiken gab?*
  a. *Falls es solche Fälle gab: Welche Maßnahmen wurden seitens des Ministeriums ergriffen?*

Allgemein ist anzumerken, dass bei jeder Technologie auch Sicherheitsrisiken bestehen. Es darf aber auf die Beantwortung der korrespondierenden Anfrage 955/J XXVII. GP der Abgeordneten Dr. Helmut Brandstätter und Douglas Hoyos-Trauttmansdorff vom 19. Februar 2020 durch den Bundeskanzler verwiesen werden.

Zur Frage 6:

- *Liegen dem Ministerium detaillierte Analysen vor, welche 5G-Komponenten aus sicherheitspolitischer Sicht Kerntechnologie darstellen, und welche nicht?*
  - *a. Wenn ja, von wem stammen diese?*
  - *b. Wenn ja, wird in diesen Analysen aufgeschlüsselt, welche dieser Komponenten ohne jegliches Sicherheitsrisiko von Huawei oder ähnlichen Unternehmen bezogen werden könnten?*
  - *c. Gibt es alternative Anbieter aus Europa, die solche Kernkomponenten in kritischen Bereichen bereitstellen könnten, oder ist man hier de facto auf chinesische Anbieter angewiesen?*
  - *d. Wenn nein, warum liegen dem Ministerium solche Analysen nicht vor?*
    - *i. Ist es geplant, Einschätzungen von Expert_innen einzuholen?*
    - *ii. Wenn ja, wann?*
    - *iii. Wenn ja, von welchen Expert_innen? Bitte um Auflistung.*

Eine Risikoanalyse in Hinblick auf potenzielle Gefahren im Zusammenhang mit der Einführung von 5G-Technologie wurde seitens der RTR-GmbH (Rundfunk und Telekom Regulierungs-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 (https://www.rtr.at/de/tk/5GCybersicherheitsanalyse2019).

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

Im Übrigen wird darauf hingewiesen, dass diese Fragen nicht in den Vollzugsbereich des Bundesministeriums für Inneres fallen und sich somit einer Beantwortung entziehen. Es

darf auf die Beantwortung der korrespondierenden Anfrage 952/J XXVII. GP der Abgeordneten Dr. Helmut Brandstätter und Douglas Hoyos-Trauttmansdorff vom 19. Februar 2020 durch die zuständige Bundesministerin für Digitalisierung und Wirtschaftsstandort verwiesen werden.

Karl Nehammer, MSc

	Datum/Zeit	2020-04-17T15:39:18+02:00
	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	2020-04-17T15:43:02+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.	