951/J
vom 19.02.2020 (XXVII. GP)

Anfrage

der Abgeordneten Dr. Helmut Brandstätter, Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen

an die Bundesministerin für Landesverteidigung

betreffend Crypto und 5G

Am 11. Februar 2020 enthüllte die Washington Post, dass das Schweizer Unternehmen Crypto weltweit jahrzehntelang Verschlüsselungssysteme verkaufte, die es den Nachrichtendiensten CIA und BND erlaubte, Nachrichten mitzulesen. Einige Zeit lang stand Crypto sogar im Eigentum dieser beiden Geheimdienste. Auch Österreich war ein Crypto Kunde. Es ist anzunehmen, dass Regierungen Verschlüsselungssysteme, mit denen sie ihre Geheimnisse kommunizieren, harten Tests unterziehen. Dennoch wurden kompromittierte Crypto Systeme jahrzehntelang an etwa 120 Staaten verkauft.
Wie viele andere Staaten ist Österreich im Moment dabei, den Aufbau seines 5G-Kommunikationssystems zu planen. Auch hier steht nun seit geraumer Zeit die Frage im Raum, ob wir dem Hersteller jener Technologie, auf die unser Kommunikationssystem der Zukunft aufgebaut sein wird, trauen können.

Im Hinblick auf den Ausbau des 5G-Netzes ergeben sich neben sicherheitspolitischen selbstverständlich auch technische Fragen. Die Novellierung des Bundesministeriengesetzes erschwert die Beurteilung der Zuständigkeiten hinsichtlich der verschiedenen problematischen Aspekte des 5G-Ausbaus noch zusätzlich.

Die unterfertigten Abgeordneten stellen daher folgende

Anfrage:

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?
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?
3. 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?
4. 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?

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?
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.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-02-19T14:36:51+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.	