Stiftung
Neue
Verantwortung

Auswärtiger Ausschuss, 13.03.2019
Fachgespräch zur Einführung des Mobilfunkstandards 5G

Session II: Einflussmöglichkeiten ausländischer Staaten auf in Deutschland tätige Netzwerkausrüster und Kontrollmöglichkeiten des deutschen Staates

Industriespionage

- In der Vergangenheit waren Mobilfunknetze (3G/4G) für Industriespionage **kein relevanter Angriffsvektor**. Infizierte E-Mails sind deutlich effizienter.
- 5G-Netze werden zwar potenziell "interessantere" Daten transportieren, aber es ist fraglich ob 5G-Netze zukünftig leichter zu hacken sind, als die IT in Unternehmensnetzwerken. (Nur dann würden Angreifer ihren Fokus verlagern)
- **Verschlüsselung** auf Applikationsebene erschwert Spionage erheblich und kann unabhängig von Hersteller und Betreiber zum Einsatz kommen.

Sabotage (Konfliktfall)

- Die effektive Störung der Kommunikationsnetze im Konfliktfall ist technisch extrem aufwendig und äußerst unwahrscheinlich.
- Risiko kann durch Heterogenität in der Netzwerkarchitektur, Redundanz und **Sicherheitsanforderungen an den Netzbetreiber** minimiert werden.
- Staatliche Akteure werden im Konfliktfall immer versuchen die Kommunikation zu stören – unabhängig vom Hersteller sollte beim Betrieb von TK-Netzen dieses Risiko adressiert werden. (siehe Arbeit in Großbritannien von NCSC)

Technologische Abhängigkeit

- 5G ist erst der Anfang, da chinesische Unternehmen eine immer stärkere Rolle in verschiedensten Technologien, gerade im Bereich IKT, spielen. Ähnliche Debatten werden in anderen Sektoren / Technologien folgen.
- Es bräuchte eine **sektorspezifische Analyse** der Abhängigkeit von außer-europäischem Equipment aus sicherheits-, industrie- und außenhandelspolitischer Perspektive.
- Ziel: Identifikation von Technologien und Positionen innerhalb der Lieferkette, die durch Europa weiterhin oder zukünftig besetzt werden sollten, um einer **technologischen Abhängigkeit** entgegenzuwirken.

Jan-Peter Kleinhans | Projektleiter IT-Sicherheit im Internet der Dinge | jkleinhans@stiftung-nv.de