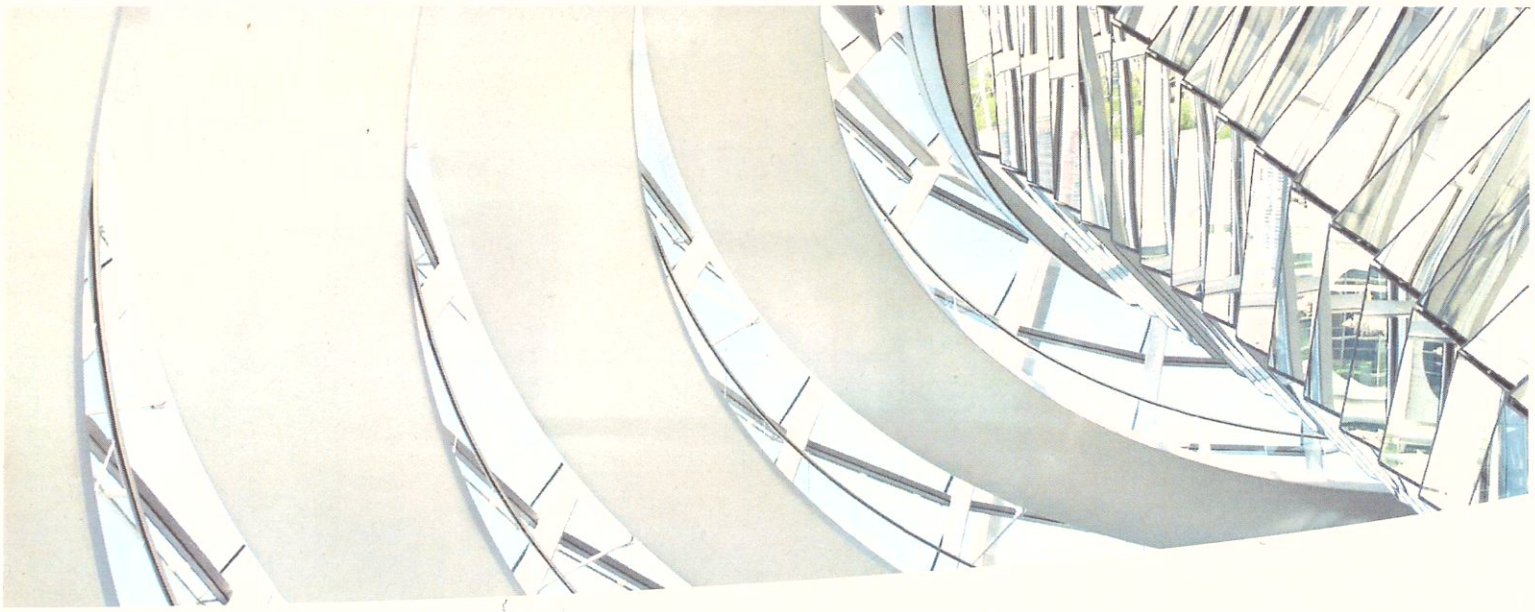

Deutschlands digitale Souveränität sichern – Maßstäbe für sichere 5G-Netze setzen

Positionspapier der
CDU/CSU-Fraktion im Deutschen Bundestag

Entwurf vom 10. Februar 2020

CDU CSU
Fraktion im Deutschen Bundestag

5G-Netzen kommt eine zentrale Bedeutung im digitalen Transformationsprozess unserer Wirtschaft und Gesellschaft zu. Sie werden in Zukunft ein breites Spektrum an Anwendungen möglich machen, die weit über die heute bekannten Formen mobiler Kommunikation hinausgehen, und damit Grundlage für viele Entwicklungen des 21. Jahrhunderts sein.

Um das Potential dieses Transformationsprozesses zur Entfaltung zu bringen und gleichzeitig unsere Wirtschaft und Gesellschaft vor Diebstahl, Sabotage, Manipulation und Einflussnahme im Netz zu schützen, müssen die kommenden 5G-Netze höchsten Sicherheitsanforderungen genügen und höchste Ansprüche an Vertraulichkeit, Verfügbarkeit und Integrität erfüllen. Es gilt insbesondere zu verhindern, dass sie dem Zugriff anderer Staaten unterliegen.

5G-Netze sind Teil der kritischen Infrastruktur Deutschlands und unterliegen besonders hohen Anforderungen. Bei der Frage, ob der Datenfluss in diesen Netzen manipuliert, kontrolliert oder sabotiert werden kann und seine Inhalte anderen Staaten zugänglich sind, geht es um nicht weniger als die Autonomie und Souveränität unseres Landes. Die Sicherheit dieser kritischen Infrastruktur muss Priorität haben. Der mit Blick auf unsere wirtschaftspolitischen Ziele dringend erforderliche rasche Aufbau der 5G-Netze und ihre flächendeckende Verfügbarkeit sind mit den nationalen Sicherheitsinteressen in Einklang zu bringen.

Unsere Sicherheitsbehörden weisen darauf hin, dass der technischen Überprüfung und Überwachung eines so komplexen und dynamischen Systems wie eines 5G-Netzes Grenzen gesetzt sind. Hierzu gehört beispielsweise die verlässliche Prüfung von vielen Millionen Zeilen Systemcode oder eines Softwareupdates, mit dem unter Zeitdruck in einem System Sicherheitsrisiken behoben werden müssen. Darüber hinaus ist davon auszugehen, dass staatliche Akteure mit entsprechend großem Ressourceneinsatz das Netzwerk jedes Herstellers infiltrieren können. Sicherheitsrisiken können demnach trotz umfassender technischer Überprüfung nicht vollständig eliminiert, sondern allenfalls minimiert werden.

Gleichwohl sind wir dem Versuch, Daten in 5G-Netzen auszuspähen, nicht wehrlos ausgeliefert. Der Einsatz einer starken Kryptographie und einer Ende-zu-Ende-Verschlüsselung bietet die Möglichkeit, die Vertraulichkeit der Kommunikation und der ausgetauschten Daten zu wahren.

Aktuell ist nicht jeder Teil des bestehenden Mobilfunknetzes gleich sensitiv und kritisch. Allerdings ist davon auszugehen, dass mit dem fortschreitenden Ausbau der 5G-Netze wesentliche Steuerungsfunktionen aus dem klassischen Kernnetz in periphere Bereiche des Netzes verlagert werden und somit neue Gefährdungen entstehen. Deshalb müssen geeignete Sicherheitsanforderungen an Zugangs-, Transport- und Kernnetz gestellt werden.

Unsere Sicherheitsbehörden machen zudem darauf aufmerksam, dass unsere 5G-Netze von zahlreichen unterschiedlichen, staatlichen und nichtstaatlichen

Akteuren attackiert werden. Sicherheit setzt Diversifikation voraus. Monokulturen, in denen eine Schwachstelle das gesamte Netz öffnet, sind auszuschließen.

Zentrales Ziel unserer Politik muss es sein, in Deutschland weltweit den Maßstab für sichere 5G-Netze zu setzen.

Die Bundesregierung ist aufgefordert, zügig die Novelle des Telekommunikationsgesetzes und das IT-Sicherheitsgesetz 2.0 vorzulegen, in denen klargestellt wird, welche Anforderungen an Sicherheit und Vertrauenswürdigkeit Telekommunikationsausrüster erfüllen müssen, um sich am 5G-Netzausbau in Deutschland beteiligen zu dürfen. Vertrauenswürdig können in diesem Zusammenhang nur solche Ausrüster sein, die einen klar definierten Sicherheitskatalog nachprüfbar erfüllen, der auch beinhaltet, dass eine Einflussnahme durch einen fremden Staat auf unsere 5G-Infrastruktur ausgeschlossen ist.

Die Bundesregierung ist darüber hinaus aufgefordert, sich auf europäischer Ebene für einen einheitlichen, hohen 5G-Sicherheitsstandard einzusetzen, dabei soll für Deutschland und analog für alle anderen Mitgliedsstaaten folgendes gelten:

Für kritische Komponenten müssen höchste Sicherheitsanforderungen gelten. Die Sicherheitsanforderungen werden über den Sicherheitskatalog definiert und von den zuständigen Bundesbehörden angewendet und kontrolliert. Der Einsatz von Komponenten eines Ausrüsters kann untersagt werden, wenn festgestellt wurde, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, entgegenstehen.

Bei Planung und Aufbau der Netze sind aus Sicherheitsgründen „Monokulturen" durch den Einsatz von Komponenten unterschiedlicher Hersteller zu vermeiden. Es ist sicherzustellen, dass ein sofortiger Umstieg auf 5G nicht gefährdet wird und eine umfassende Versorgung entsprechend der 4G- und 5G-Auflagen aus der Frequenzvergabe aus dem Jahr 2019 erfolgen kann. Für Bestandskomponenten, die nicht mehr neu verbaut werden, wird keine nachträgliche Zertifizierung verlangt. Erhält eine bereits im Netz eingesetzte kritische Komponente keine Zertifizierung oder verliert sie diese, muss die Komponente bis 2025 im Netz ersetzt werden.

Wir wollen die Erforschung und Entwicklung von kryptographischen Sicherheitstechniken und den Einsatz von flexibel einsetzbarer Mobilfunknetztechnik (Open-RAN) vorantreiben und hierfür kurzfristig prüfen, ob der am 10. November 2019 im Koalitionsausschuss beschlossene Beteiligungsfonds für Zukunftstechnologien bei der Kreditanstalt für Wiederaufbau mit aufwachsend bis zu zehn Milliarden Euro dazu einen unterstützenden Beitrag leisten kann.

Deutschland muss gemeinsam mit seinen europäischen Partnern eine Industriestrategie ausarbeiten, die sich zum Ziel setzt, europäische Unternehmen dauerhaft in den Stand zu setzen, ein international konkurrenzfähiges und sicheres 5G-Netz in allen Teilen bereitzustellen und aufzubauen, sowie sie gegen feindliche Übernahmen aus dem Ausland zu schützen. Dabei muss geprüft werden, wie

entsprechende Kompetenzen auch wieder in Deutschland aufgebaut werden können. Dies gilt entsprechend auch für andere IT-Infrastrukturen mit hohen Sicherheitsanforderungen.

Sollte ein Unternehmen gegen Sicherheitsauflagen und -anforderungen verstoßen, muss das erhebliche, auch rückwärtsgewandte Sanktionen einschließlich der Entziehung des Sicherheitszertifikates nach sich ziehen.

Für die 5G-Zertifizierung müssen europaweit einheitliche hohe Standards gelten.

Herausgeber: CDU/CSU-Fraktion im Deutschen Bundestag
Michael Grosse-Brömer MdB
Stefan Müller MdB
Platz der Republik 1
11011 Berlin