Fraunhofer

POSITIONSPAPIER DER FRAUNHOFER-GESELLSCHAFT

5G – NETZE UND SICHERHEIT

INHALT

1 EXECUTIVE SUMMARY

Die Einführung von 5G bringt neue, innovative Anwendungen und Geschäftsmodelle mit sich. Werden heutzutage nur etwa 5 Prozent des Datenvolumens in Deutschland über Mobilfunk übertragen, so wird der Standard 5G mit seinem reduzierten Energieverbrauch, der hohen Bandbreite sowie der Möglichkeit, Geräte und Maschinen untereinander in Echtzeit zu vernetzen, neue Maßstäbe setzen und das mobil übertragene Datenvolumen deutlich in die Höhe treiben. 5G-Netze befinden sich weltweit im Aufbau. Wichtige Treiber für Innovationen sind die 5G-Campusnetze, die lokal installiert werden und Firmen neue Möglichkeiten für die effiziente Steuerung ihrer Abläufe eröffnen.

Die Hersteller der 5G-Netz-Komponenten nehmen eine strategische Schlüsselposition ein. Daraus resultiert die vielfach diskutierte hohe Abhängigkeit der Netzbetreiber von den Herstellern solcher Komponenten, wie beispielsweise Huawei. Diese wiederum sind auf Cutting Edge Mikroelektronik-Hardware angewiesen, die nur wenige Hersteller beherrschen, die derzeit überwiegend aus den USA stammen. Die in 5G-Netzen sehr wichtige Software ist in hohem Maße durch Patente geschützt. Diese Software entsteht in einer Lieferkette, in der zahlreiche einzelne Software-Komponenten aus unterschiedlichen Quellen zu einer komplexen Gesamtlösung zusammengefügt werden. Hintertüren und Einfallstore können dadurch bislang – selbst wenn sie entdeckt werden – kaum eindeutig einem Urheber zugeordnet werden.

Somit entstehen mit 5G vielfältige Herausforderungen und Abhängigkeiten, denen adäquat begegnet werden muss. Besonderes Augenmerk sollte dabei auch den Endgeräten gelten. Darüber hinaus darf nicht vergessen werden, dass auch in konventionellen Systemen hohe Risiken durch staatliche Einflussnahme, insbesondere zum Zweck der Spionage und Sabotage, bestehen. Dieses Potenzial wird mit 5G aufgrund der vielfältigen Einsatzmöglichkeiten sowie dem möglichen Einsatz in sicherheitskritischen Bereichen noch beträchtlich höher sein, sofern keine geeigneten Schutzvorkehrungen getroffen werden.

Fraunhofer spricht acht Empfehlungen aus, die zum einen kurz- und mittelfristig eine Erhöhung der 5G-Sicherheit versprechen und langfristig auf eine Stärkung der technologischen Souveränität bei 5G abzielen. Ein Verbot einzelner Hersteller, wie es derzeit diskutiert wird, kann zur Risikoreduktion beitragen. Das Risiko vollständig beseitigen kann es nicht. Zudem könnte die damit verbundene Reduktion des Angebots kurz- und mittelfristig zu problematischen Engpässen bei der Bereitstellung von 5G führen und die Wettbewerbsfähigkeit Deutschlands als Forschungs- und Innovationsstandort empfindlich beeinträchtigen.

Unmittelbar umzusetzende Maßnahmen (kurz- bis mittelfristige Perspektive):

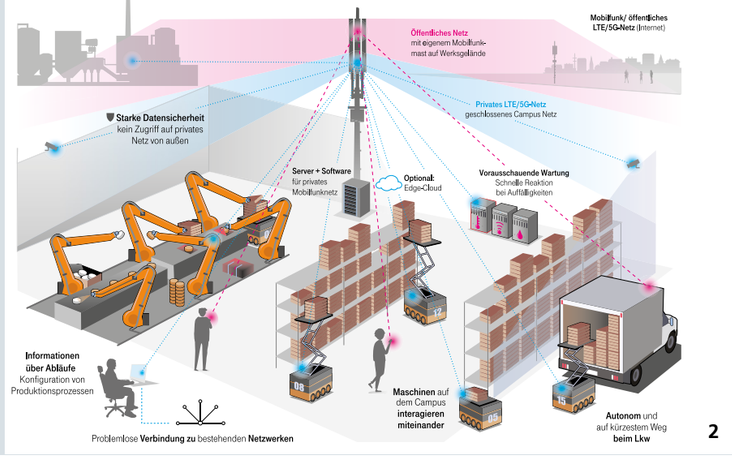
1. **Sichere Ende-zu-Ende-Verschlüsselung:** Wir empfehlen, den flächendeckenden Aufbau von PKI-Infrastrukturen für eine Ende-zu-Ende-Verschlüsselung auf deutscher und EU-Ebene schnell und effektiv zu fördern.
2. **Konsequentes Prüfen und Zertifizieren:** Die Politik sollte schnellstmöglich geeignete Prüfkriterien und Prüfmaßnahmen aufstellen, sowie den Aufbau von Prüflaboren vorantreiben.
3. **Aufbau von gesicherten Campusnetzen:** Die Politik sollte deutsche Unternehmen und Start-ups fördern, die entsprechende Lösungen bereitstellen, und sich so einen Wachstumsmarkt erschließen.
4. **Sichere Endgeräte:** Die Politik sollte Anreize schaffen, die Absicherung von Endgeräten zu fördern.
5. **Europäisches Konsortium zur Stärkung der Marktposition von Nokia und Ericsson:** Europa sollte schnell agieren, um möglichen Kontrollverlusten zuvorzukommen.
6. **Nutzung konventioneller Netze für sicherheitskritische Anwendungen:** Wir empfehlen für hohe Sicherheitsanforderungen nur EU-Netzkomponenten zu nutzen.

Stärkung der technologischen Souveränität (langfristige Perspektive):

1. **Entwicklung von 5G-Komponenten in Europa:** Wir empfehlen die Umsetzung einer umfassenden Forschungsstrategie für die Entwicklung von 5G-Komponenten. Der Finanzbedarf hierfür wird auf einen ein- bis zweistelligen Milliarden-Euro-Betrag geschätzt.
2. **Initiierung einer »Open 5G Partnership Initiative« Europe:** Wir empfehlen die Entwicklung einer 5G-Referenzplattform sowie die Etablierung von Communities, die offene Software für 5G entwickeln und betreiben.

Fraunhofer kann bei allen genannten Maßnahmen substantiell unterstützen, u. a. durch

- **Nutzung der Fraunhofer-Testlabore** zur schnellen Ausarbeitung von Prüfkriterien, Prüfmaßnahmen und zum Aufbau dedizierter 5G-Prüflabors sowie zur Ausbildung von Fachpersonal.
- **Beratung beim Aufbau und Betrieb von 5G-Campusnetzen** basierend auf bestehenden umfangreichen Erfahrungen in Reallaboren.
- **Absicherung von 5G-Endsystemen** u. a. mit Lösungen aus dem Industrial Data Space (IDS).
- **Unterstützung bei der Etablierung von Konsortien** für offene Schnittstellen-Entwicklung und Entwicklung von offenen Referenzarchitekturen.



2

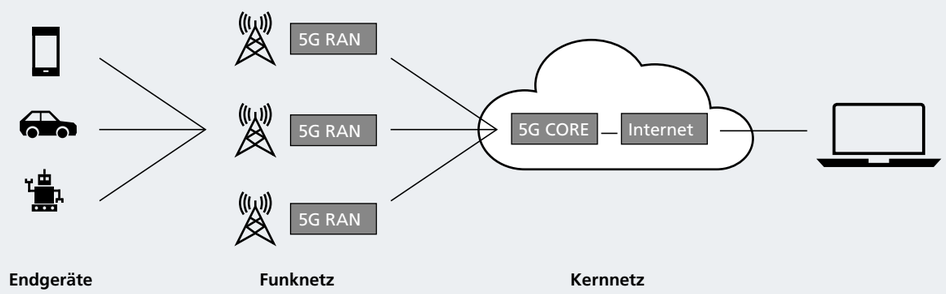
2 5G-NETZE

Ein Mobilfunknetz besteht aus drei primären Segmenten: den Endgeräten, dem Funknetz (Radio Access Network, RAN) und dem Kernnetz (Core Network, CN). Das Funknetz besteht aus Basisstationen mit den dazugehörigen Antennen. War der bisherige Mobilfunk der vierten Generation (LTE) geprägt durch eine Datenübertragung von multimedialen und anderen Inhalten von und zu den Endgeräten (in der Regel Smartphones), kommen im 5G-Netz in großem Maßstab neue Endgeräte hinzu. In der Architektur der Netze wird ein Paradigmenwechsel stattfinden: Viel stärker als bisher wird dieses einen Baukasten-charakter haben. Dies wird es erlauben, Netzinfrastrukturen flexibel aufzubauen und mittels einer Konfiguration über Software für unterschiedlichste Einsatzszenarien zu befähigen.

Die Funktionen des Kernnetzes, inklusive der Übergänge in andere Netze, werden mittels einer komplexen Software-Architektur umgesetzt. Zu beachten ist, dass heute der mit Abstand größte Teil des Datenvolumens, derzeit 95 Prozent, noch über das Festnetz übertragen wird.[1] Dies kann sich aber innerhalb der nächsten Jahre deutlich ändern, wenn der Aufbau des 5G-Mobilfunknetzes abgeschlossen sein wird. Es ist daher von größter Wichtigkeit, frühzeitig in der derzeitigen Konzept- und Aufbauphase gestaltenden Einfluss auf den Netzausbau zu nehmen.

Die in Deutschland im Aufbau befindlichen 5G-Netze werden aktuell nicht »stand-alone« aufgebaut. In einem ersten Schritt werden die bestehenden 4G-Netze um 5G-Funk-Komponenten erweitert. Charakteristisch für 5G ist eine deutlich stärkere Software-Orientierung sowie der Einsatz von Virtualisierungstechnologien. Das Kernnetz wird hierzu aus Software-Funktionsmodulen aufgebaut und kann individuell gemäß den Anwendungsanforderungen (Mobilitätsunterstützung, Dienstgüte) angepasst sowie nach Bedarf um neue Software-Funktionen

Schematische Darstellung eines 5G-Netzes



1 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2019/JB2018.pdf

ergänzt und erweitert werden. Die Virtualisierung ermöglicht die Reduktion des Anteils an spezialisierter Hardware, die bisher die digitale Signalverarbeitung im RAN und die Netzwerkfunktionalitäten im Kernnetz übernommen hat. Dadurch sind Software-basierte Ansätze auf handelsüblichen Rechnerplattformen möglich. Die Aufteilung des Funknetzes in zentrale Steuereinheiten und verteilte intelligente Antenneneinheiten erleichtert zudem die Diversifikation der Komponenten-Lieferanten. 5G-Technologien unterstützen Anwendungen mit sehr unterschiedlichen Anforderungsprofilen: von Multimedia-Anwendungen, die die Übertragung sehr großer Datenvolumina erfordern, über IoT-Netze, bei denen eine sehr große Anzahl von Endgeräten angeschlossen werden, bis hin zu Anwendungen, in denen Daten in Echtzeit übertragen werden müssen. Es wird daher auch viele unterschiedliche 5G-Netz-Ausprägungen geben. Durch Netzwerk-Slicing (Bereitstellung virtueller Overlay-Netze) gibt es zudem die Möglichkeit, Dienste mit sehr unterschiedlichen Qualitätseigenschaften über das gleiche physikalische Netz eines Netzbetreibers abzuwickeln.

5G soll durch seine Leistungsmerkmale die verschiedensten Anwendungen der digitalen Transformation effizient unterstützen, d.h. es wird eine enge Verzahnung von 5G-Kommunikation, Datenverarbeitung und Anwendungsausführung (Sensorik, Aktuatorik) geben. Daher wird auch den 5G-Endgeräten – das sind insbesondere Maschinen, bemannte und unbemannte Fahrzeuge und IoT-Geräte – eine sehr große Bedeutung zukommen. Das Angebot an Endgeräten ist breit gefächert und erlaubt den Anwendern einerseits eine Diversifizierung; andererseits können bei vielen Endgeräten individuelle Absicherungslösungen gegen ein Abhören der Kommunikation implementiert werden, z.B. durch eine sichere Ende-zu-Ende-Kommunikation.

Eine weitere wichtige Neuerung, die 5G mit sich bringt, ist die Möglichkeit, wahlweise öffentliche oder private 5G-Campusnetze (Abbildung 2) aufzubauen. Diese Netze bedienen die Bedürfnisse der Betreiber nach lokaler Datenhaltung (Datensouveränität), nach einer drahtlosen Anbindung an die Unternehmensnetze sowie Echtzeitkommunikation. Ermöglicht werden diese Neuerungen durch den Einsatz von sogenannten Small Cells (Funkzellen mit geringerer Leistung aber höherer Standortdichte) sowie von dedizierten, lokal betriebenen Kernnetzen. Damit kann die Industrie ihre Daten direkt in eigenen lokalen Datenzentren (Edge Cloud) verarbeiten, statt sie über das öffentliche Mobilfunknetz zu übertragen. **Deutschland gilt weltweit als Pionier bei der frühen Vergabe von lokalen 5G-Frequenzen.** Als erste industrielle 5G-Ausprägungen stellen Campusnetze daher frühzeitig sehr hohe Anforderungen an Datensicherheit und Ausfallsicherheit.

Um die mit der Einführung von 5G-Netzen verbundenen Risiken zu kennen, ist es erforderlich, die wichtigsten Abhängigkeitsbeziehungen und die daraus resultierenden möglichen Risiken zu erfassen. Nachfolgend stellen wir die Sicht der Fraunhofer-Gesellschaft dar und leiten Handlungsoptionen und -empfehlungen zur Reduktion der Risiken ab. Die Empfehlungen der Fraunhofer-Gesellschaft sind als eine Ergänzung des Ende Januar 2020 erschienenen Berichts der EU, der sogenannten 5G-Toolbox, zu sehen. Darin wurden die Ergebnisse einer 2019 durchgeführten Befragung unter den EU-Mitgliedsstaaten zusammengestellt und Empfehlungen für zu ergreifende Maßnahmen zur Sicherheit in 5G-Netzen abgeleitet.

2 *Infografik Campus-Netze »Die Campus-Lösung«, © Deutsche Telekom https://www.telekom.com/de/konzern/details/ 5g-technologie-in-campus-netzen-556690*

3 ABHÄNGIGKEITEN

Um zu einer fundierten Risikobewertung zu gelangen, ist es wichtig, die vielschichtigen Abhängigkeiten zu verstehen, die sich mit dem neuen Eigenschaftsprofil der 5G-Infrastrukturen ergeben.

- **Technologische Abhängigkeit der Netzbetreiber von Komponenten-Herstellern beim Betrieb der Netze.** Der 5G-Netzmarkt wird aktuell von drei Anbietern von Netzkomponenten dominiert: Huawei, Ericsson und Nokia. Daneben spielen auch ZTE und Samsung eine zunehmend bedeutsame Rolle. Die Marktanteile von Huawei und ZTE betragen zusammen ca. 40 Prozent, jene von Nokia und Ericson zusammen 31 Prozent, der Rest des Markts wird von spezialisierten Anbietern abgedeckt. Huawei ist Technologieführer und hat insbesondere im Funknetz-Bereich aktuell eine dominierende Stellung. Auch im eng mit dem 5G-Netzmarkt verwobenen Markt für 5G-Modemchips gibt es nur noch wenige Anbieter: Qualcomm, HiSilicon (Huawei), Samsung, MediaTek, Sequans (bisher nur LTE) sowie künftig auch Apple (als Käufer der Intel Modem-Sparte). Mit Ericsson (Schweden) und Nokia (Finnland) ist Europa im Infrastrukturteil vergleichsweise gut vertreten, im Modembereich (mit Sequans, Frankreich) jedoch eher schwach.

- **Technologische Abhängigkeit der Komponenten-Hersteller** (Router, Switches) **von ihren Technologie-Zulieferern** (Modemchipsätze, Transceiver). Alle derzeit am Markt dominierenden Hersteller von Netzkomponenten sind gleichermaßen von Zuliefer-Produkten abhängig, die derzeit von Unternehmen aus den USA dominiert werden, wie beispielsweise den Weltmarkführern für Transceiver Lumentum und Finisar / II-VI. Die US-amerikanischen Zulieferer lassen jedoch ihrerseits in China und Malaysia fertigen, wodurch eine Supply-Chain-Abhängigkeit (s.u.) entsteht. Chinesische Hersteller sind derzeit nur im Low-Cost-Zuliefererbereich tätig, wodurch sich bemerkenswerte wechselseitige Abhängigkeiten zwischen der US-amerikanischen Zuliefer-Industrie, chinesischen Netzkomponentenherstellern und Netzwerkbetreibern ergeben. Aufgrund der aktuell in den Medien verlautbarten Einschätzungen der US-amerikanischen Regierung hinsichtlich der Vertrauenswürdigkeit chinesischer Hersteller ist zu erwarten, dass die US-amerikanischen Zulieferer mittelfristig außerhalb Chinas produzieren werden.

- **Technologische Abhängigkeit der Netzbetreiber und Komponenten-Hersteller von komplexen Software-Modulen und Software-Stacks** für Virtualisierung (u. a. Network Function Virtualization (NFV)) und für die Software-Orientierung (u. a. Software-Defined-Networking (SDN)). Neben proprietärer Software der Hersteller entwickeln sich erste Ansätze für offene Lösungen mit klar spezifizierten Schnittstellen für die Systemkomponenten sowie dazugehörige Open Source-Referenzimplementierungen. Beispiele dafür sind die Telefonica Open Source Mano (OSM)-Realisierung des ETSI NFV Management and Orchestration (MANO) Software Stacks sowie die Open RAN-Allianz (http://www.oran.org) und der dazugehörige Open Source Software-Stack für den Funkzugang (RAN). Diese Entwicklung betrifft aber – bisher noch – nicht das Kernnetz.

- **Technologische Abhängigkeit aller Beteiligter von der gesamten Hardware- und Software-Supply-Chain.** Es bestehen allein hardwareseitig hohe Abhängigkeiten, da sowohl die Netzausrüster auf ihre US-amerikanisch dominierten Zulieferer, als auch die Zulieferer ihrerseits auf die Fertigungsstandorte – vielfach in China – angewiesen sind. Eine hohe Abhängigkeit ergibt sich außerdem für die Software-Supply-Chain, da komplexe Software aus vielen Software-Paketen aus unterschiedlichen Quellen erstellt und auch Standard-Software-Komponenten (wie z.B. Software-Bibliotheken) wiederverwendet werden.

- **Technologische Abhängigkeit von Standard-Hardware-Technologie** für die mittels Glasfaser angebundenen Cloud- und Edge-Cloud-Plattformen. Hier bestehen die gleichen Abhängigkeiten wie für alle IT-basierten Anwendungen. Design und IPs (z.B. von Intel, AMD, ARM) können in USA und Europa beheimatet sein, die Herstellung erfolgt zu einem überwiegenden Teil in Asien (Korea, Taiwan).

- **Technologische Abhängigkeit der neuen 5G-Netze von Bestandsystemen,** also 3G und 4G. Bestehende 4G-Netze werden um eine 5G-Funkkomponente erweitert, d.h. die verbauten 4G-Komponenten werden weiterhin benötigt.

- **Technologische Abhängigkeit der Nutzer** (Industrie, Staat, Bürger) von Endsystemen.

- **Politische Abhängigkeit durch staatliche Einflussnahmen auf nationale Hersteller mittels u. a. nationaler Gesetzgebung, die mittelbare Auswirkungen auf Deutschland haben würde.** Staaten können zum Beispiel über gesetzliche Vorschriften Druck auf ihre nationalen Hersteller ausüben und somit die Möglichkeiten für staatliche Angriffe unterstützen oder initiieren und damit im technischen Sinne zu Angreifern werden. Das betrifft Huawei, aber auch viele andere Hersteller, auch solche, deren Komponenten sich in den Komponentenlisten nicht-chinesischer Hersteller befinden.

4 RISIKEN

Aus den skizzierten Abhängigkeitsstrukturen ergeben sich unmittelbar wesentliche Risiken für 5G-Netze. Besonders relevant sind intrinsische Risiken, diese können einerseits durch den Aufbau, durch technische Schwachpunkte oder Schwächen bei der Umsetzung des 5G-Netzes, oder andererseits durch willkürliche oder unwillkürliche eingebaute Fehler entstehen. Die 5G-Technologie eröffnet durch ihre neuen Anwendungsfelder zusätzlich auch verstärkt das Risiko für gezielte Angriffe von außen.

Das Verfügbarkeitsrisiko wird im Folgenden bewusst ausgeklammert. Netzausfälle sind generell nicht auszuschließen, daher müssen 5G- und andere Netzanwendungen (z.B. im Energiesektor oder Automotive-Umfeld) auf Netzausfälle vorbereitet werden, beispielsweise durch autonome Notsteuerungen und redundante Netzauslegungen.

Biologische Risiken, die durch elektromagnetische Strahlung entstehen, werden in diesem Positionspapier bewusst ausgeklammert. Für Fragen zu diesem Themenkomplex bietet sich unter anderem das Bundesamt für Strahlenschutz (BfS) als Ansprechpartner an. Das BfS plant zur Bearbeitung derartiger Fragestellungen den Aufbau eines Kompetenzzentrums Elektromagnetische Felder in Cottbus.

Ebenso wenig werden in diesem Papier die derzeitige **Patentsituation und Patentpolitik**, sowie mögliche Geschäftsmodelle, u. a. der USA, adressiert, da die Auswirkungen, die sich hieraus ergeben könnten, bisher noch sehr spekulativ sind.

4.1 Risiko Hersteller

Hersteller, die ihre jeweiligen Netzkomponenten bewusst mit korrumpierter Hardware oder Software ausstatten, indem u.a. Hintertüren als Hardware- oder Software-Trojaner integriert werden, können Daten im 5G-Kernnetz, RAN und in Endgeräten ausspähen und Sabotage-Angriffe durchführen. Die Daten werden bei 5G zwar bei der Übertragung über das Funknetz sowie bei der Übertragung zwischen Netzwerkbetreibern beim Roaming verschlüsselt, im Kernnetz jedoch werden sie offen auf den jeweiligen Komponenten verarbeitet.

Mit den heute vorliegenden Methoden können Hardwarekomponenten und Zulieferer-Komponenten sehr detailliert sowohl auf vorhandene als auch auf versteckte Funktionalitäten sowie mögliche Schwachstellen untersucht werden. Auch bei der Analyse von Software, insbesondere bei Vorlage von Source-Code, kann mit heutigen Verfahren bereits sehr tiefgehend analysiert und geprüft werden.

Bei komplexen (Software)-Systemen kann alleine mit statischen, einmaligen Tests das Vorhandensein von Hintertüren und Schadcodes nicht mit ausreichend hoher Wahrscheinlichkeit ausgeschlossen werden. Dies trifft auf alle Produkte aller Hersteller zu. Es ist daher unabdingbar, dass alle Komponenten aller Hersteller, die in kritischen Netzbereichen zum Einsatz kommen, kontinuierlich und systematisch getestet und analysiert werden.

4.2 Risiko Software

Software nimmt eine bedeutende Rolle bei 5G-Architekturen ein. Daher sind die Risiken, die sich durch Software ergeben können, beträchtlich. In der Vergangenheit wurden die Schwachstellen in Software als **primäres Einfalltor für Cyberangriffe** genutzt. Praktisch alle großen Software-Systeme ent-

halten solche Schwachstellen, so dass davon auszugehen ist, dass dies auch auf die komplexen 5G-Software-Architekturen zutrifft. Da Software-Module im operativen Betrieb ausgetauscht, aktualisiert (update) oder auch angepasst (patchen) werden können, ist neben den angesprochenen systematischen und rigorosen Tests auch die engmaschige Überprüfung und Überwachung über den **gesamten Software-Lebenszyklus erforderlich.**

4.3 Risiko Supply Chain

Aus den tiefgreifenden Abhängigkeiten innerhalb der hochspezialisierten und global verteilten Zuliefer-Ketten ergeben sich aufgrund der geringen Diversifizierung weitere beträchtliche Risiken. Komplexe Software wird heutzutage nicht mehr aus einer Hand entwickelt, sondern besteht aus einer Vielzahl einzelner Software-Pakete und -Bibliotheken, die die Software-Supply-Chain ausmachen. Durch die Abhängigkeiten innerhalb der Supply-Chain ist es derzeit praktisch unmöglich, eine gefundene Schwachstelle oder eine Hintertür einem Verantwortlichen zuzuordnen (sogenannte Attributierung). Aus diesem Grund laufen auch die momentan diskutierten Haftungsregelungen ins Leere, die darauf abzielen, Hersteller, denen der Einbau von Hintertüren nachgewiesen wurde, mit existenzbedrohend hohen Strafen, z.B. in Höhe eines Jahresumsatzes, zu drohen.

4.4 Risiko Campusnetz

Campusnetze für Versorgungstrukturen, wie beispielsweise Stadtwerke oder vernetzte Industrieanlagen, können von Netzbetreibern gestellt oder privat aufgebaut werden. Bei einer mangelhaften Konfigurierung, fehlender Diversifizierung bei den eingesetzten Technologien, fehlenden Sicherheitsevaluationen der genutzten Software und mangelhaften Zugriffskontrollen können beträchtliche Angriffsflächen für gezielte Attacken (auch durch organisierte Kriminalität) eröffnet werden, die zu massiven Beeinträchtigungen bei der Versorgungssicherheit oder Schäden durch Spionage und Sabotage führen können.

4.5 Risiko Endgerät

5G-Endgeräte sind häufig Bestandteile kritischer Prozesse und Infrastrukturen, wie beispielsweise Maschinen in einer Produktionsstraße oder autonome Fahrzeuge. Anders als bei den Komponenten des Kernnetzes existiert bei den Endgeräten ein diversifiziertes Angebot an Komponenten. Daher treffen die Aussagen zu den Risiken der Software auch auf die Endgeräte zu. Daten können auf den Endgeräten vor dem Transport über das 5G-Netz Ende-zu-Ende verschlüsselt werden, so dass sie geschützt durch das gesamte 5G-Netz inklusive der unsicheren Komponenten übertragen werden. Durch das gezielte Ausbringen von Spionagesoftware auf Endgeräte könnte jedoch auch eine Ende-zu-Ende-Verschlüsselung unterwandert werden, indem die Daten bereits an der Quelle oder an der Senke abgegriffen oder modifiziert werden können. Allerdings existieren zur Absicherung von Endgeräten bereits zahlreiche einsetzbare Lösungen.

4.6 Risiko staatliche Einflussnahme

In konventionellen Systemen besteht bereits ein beträchtliches Risiko staatlicher Einflussnahme mit dem Ziel der Spionage oder Sabotage. In 5G-Netzen ist dieses Risiko ungleich höher, da aufgrund der geringen Diversifizierung und starken Software-Basierung eine solche Einflussnahme auf vielfältige Weise erfolgen kann. Die Einflussnahme über nationale Hersteller, wie im Fall Huawei, ist dabei nur eine Möglichkeit. Ein anderer Weg der gezielten Beeinflussung kann durch gezieltes Infiltrieren von manipulierten Software-Modulen, die auf Komponenten beliebiger Hersteller zur Ausführung kommen, erfolgen oder durch die Infiltrierung von Zuliefer-Technologie, von der alle Hersteller abhängig sind. Der daraus resultierende Schaden ist davon abhängig, welche Aufgaben die manipulierten Komponenten in einem Netzwerk ausüben. Gefährdete Komponenten sollten daher bewusst so eingesetzt werden, dass ein Angriff durch sie weitestgehend wirkungslos bleibt. Leider ist eine solche Härtung und Isolierung nicht immer möglich. **Der Marktausschluss eines Herstellers, wie beispielsweise Huawei, würde das Risiko der staatlichen Einflussnahme reduzieren, jedoch nicht vollständig ausschließen.** Hierfür müssten alle an zentralen Stellen verbauten Technologien ausgeschlossen werden, die aus einem Land stammen, dessen staatliche Einflussnahme man heute oder in naher Zukunft befürchtet. Allerdings gilt diese Logik im gleichen Maße bereits für 3G- und 4G-Netze sowie das Festnetz. Derzeit gibt es nur drei relevante Anbieter für die Elemente des 5G-Kernnetzes: Huawei (China) sowie Ericsson und Nokia (Europa). Daneben existieren eine Reihe kleinerer Hersteller, wie Mavenir, NEC, Samsung, Athonet, Qortus. Diese haben jedoch noch keine konkurrenzfähigen Produkte für die Ausrüstung großer Netze auf dem Markt. **Eine Reduktion des Angebots durch Ausschluss einzelner Hersteller könnte kurz- und mittelfristig zu problematischen Engpässen bei der zeitnahen Bereitstellung von 5G führen.**

5 HANDLUNGSOPTIONEN UND EMPFEHLUNGEN

Die in Abschnitt 4 dargestellten Risiken lassen sich mit unterschiedlichen Einzelmaßnahmen, besser aber noch durch ein Bündel von Maßnahmen kurz- bis mittelfristig beträchtlich reduzieren. Ende-zu-Ende-Verschlüsselung und technisch tiefe Sicherheitsprüfungen können signifikant dazu beitragen, Spionage-Risiken durch Komponenten-Hersteller, durch Zuliefer-Komponenten in den Lieferketten und durch staatliche Einflussnahmen deutlich zu reduzieren. Darüber hinaus trägt eine staatliche Unterstützung für den Aufbau sicherer Campusnetze sowie von Netzen mit sehr hohen Sicherheitsanforderungen zur weiteren Reduktion der Risiken durch Hersteller und mögliche staatliche Einflussnahmen bei. Der hohen Abhängigkeit von marktdominanten Herstellern kann durch eine systematische Förderung europäischer Lösungen begegnet werden. Um langfristig und nachhaltig alle in Abschnitt 4 aufgeführten Risiken deutlich zu verringern, wird empfohlen, erheblich in die staatliche Förderung von Forschung und Entwicklung für 5G-Komponenten inklusive der dafür erforderlichen Software zu investieren.

5.1 Unmittelbar umzusetzende Maßnahmen (kurz- bis mittelfristig)

Ein großer Teil möglicher Spionage-Angriffe kann durch den Aufbau einer sicheren Ende-zu-Ende-Verschlüsselung abgewehrt werden. Die sensitiven Daten liegen dann im 5G-Netz nicht im Klartext vor und können auch nicht direkt von einer Netzkomponente abgegriffen werden. Allerdings ist aufgrund fehlender Infrastrukturen eine flächendeckende Ende-zu-Ende-Verschlüsselung in Deutschland nicht unmittelbar realisierbar. So ist die Identifizierung (bzw. Registrierung) von Nutzern und die sichere Verteilung von Public-Key-Zertifikaten für große und vergleichsweise offene Systeme in der Praxis immer noch eine große Herausforderung. Aus diesem Grund gibt es in Deutschland auch noch immer keine flächendeckende und breit genutzte Public-Key-Infrastruktur (PKI). Die Umsetzung innerhalb eines geschlossenen Systems, wie z. B. der Belegschaft der Fraunhofer-Gesellschaft oder anderer größerer Unternehmen, ist technisch realisierbar und wird bereits eingesetzt. **Wir empfehlen, den flächendeckenden Aufbau von Public-Key-Infrastrukturen zu unterstützen. Damit wäre eine Ende-zu-Ende-Verschlüsselung prinzipiell auch alleine auf deutscher oder EU-Ebene umsetzbar.**

Eine wirksame Verschlüsselung setzt ihrerseits sichere Endgeräte voraus. Zur Absicherung von Endgeräten existieren bereits viele einsatzreife Lösungen, die insbesondere von KMUs vertrieben werden. **Die Politik sollte Anreize schaffen, um die Absicherung von Endgeräten zu fördern. Damit würde ein wichtiger und schnell umzusetzender Schritt zur Reduktion von Angriffen erfolgen.**

Risiken von Schäden durch Sabotage lassen sich mit Ende-zu-Ende-Verschlüsselung alleine nicht verringern. Mit **konsequenter Zertifizierung und Prüfung** von Software und Hardware kann aber ein substanzieller Beitrag zur Vertrauensbildung geleistet werden. Die Zertifizierung muss dabei die Sicherheit von Produkten und Herstellungsprozessen demonstrieren. Grundlage dafür ist die unabhängige Sicherheitsanalyse durch ein vertrauenswürdiges Prüflabor. Im besten Fall legt der Hersteller gegenüber dem Labor alle Details offen (z. B. Sourcecode, Entwurfsentscheidungen). Beim Testen von Hardware und Software gibt es jedoch Grenzen, Restrisiken bleiben bestehen. Dennoch kann eine Zertifizierung helfen, grobe Entwurfsfehler zu entdecken und zahlreiche Schwachstellen in der Implementierung zu beseitigen. Bei kleineren Systemen bzw. Teilsystemen kann eine Zertifizierung sogar auf formale Methoden zur Validierung und Verifikation zurückgreifen. Zu beachten ist, dass Software sich auch nach der Inbetriebnahme noch ändern kann, beispielsweise wenn sie vom Hersteller selbst mit Updates bzw. Patches aktualisiert wird (etwa zur Fehlerbehebung). **Jede Aktualisierung der Software muss also eine erneute Sicherheitsevaluierung und Aktualisierung der Zertifizierung nach sich ziehen.** Dies ist machbar, in der Praxis aber äußerst aufwändig. Zudem kann die damit verbundene Verzögerung bei den Updates leicht zu einer Verringerung der Sicherheit führen, wenn dadurch offene Schwachstellen nicht schnell genug geschlossen werden.

Die Politik sollte mit Nachdruck daran arbeiten, geeignete Prüfkriterien aufzustellen und Prüfmaßnahmen zu etablieren sowie die Entwicklung von automatisierten Prüfwerkzeugen voranzutreiben. Auch mit dem zügigen Auf- und Ausbau von kompetenten Prüflaboren mit den erforderlichen Ausstattungen sollte umgehend begonnen werden.

Die Darstellung der Abhängigkeiten und Risiken verdeutlicht, dass für sicherheitskritische Anwendungen alternative, ggf. ausschließlich mit konventioneller Glasfaser und Funktechnologie ausgelegte, bestmöglich abgesicherte Netze oder sogar spezielle eigene Netze, wie aus dem Behördenbereich bekannt, genutzt bzw. aufgebaut werden sollten.

Wir empfehlen für hohe Sicherheitsanforderungen keine Netzkomponenten zu nutzen, die nicht aus der EU stammen. Damit sind jedoch die Abhängigkeiten, die sich aus den Zuliefer-Ketten ergeben, noch nicht beseitigt. Eine ganzheitliche Evaluierung und Prüfung der genutzten Hardware- und Software-Komponenten über den gesamten Lebenszyklus ist daher unabdingbar.

Wir empfehlen den Aufbau von gesicherten Campusnetzen, die großes Potenzial haben, die Vorteile der 5G-Technologie gesichert und kontrolliert für industrielle Anwendungen nutzbar zu machen. Die Politik sollte gezielt den Aufbau solcher Netze unterstützen, indem Unternehmen gefördert werden, die hierfür entwickelte Lösungen bereitstellen.

Dies kann einen großen Anreiz für deutsche oder europäische Start-ups darstellen, sich als alternative Lieferanten mit innovativen Lösungen einen Wachstumsmarkt zu erschließen. Derzeit haben Nokia und Ericson zusammen einen Marktanteil von nur ca. 31 Prozent. Die chinesischen Anbieter haben den immensen Vorteil eines riesigen Binnenmarkts, der für Infrastrukturanbieter essentiell ist. China ist ein Early Adopter von 5G. 2019 wurden bereits 130 000 Funkmasten von 4G auf 5G für ca. 500 Mio USD umgestellt. Da 5G-Modemchipsätze in der extrem teuren 7-nm-Technologie mit Einmalkosten im Milliarden-Euro-Bereich hergestellt werden, ist Marktgröße bei 5G deutlich wichtiger als bei 3G und 4G. Derzeit gibt es in den USA Überlegungen, sich an Nokia oder Ericson zu beteiligen, um Kontrolle zu erhalten. Hier sollte Europa frühzeitig gegensteuern, damit die Kontrolle nicht vollständig an nicht-europäische Länder abwandert.

Wir empfehlen deshalb, die Marktstellung der europäischen Hersteller Nokia und Ericson deutlich zu stärken.

5.2 Stärkung der technologischen Souveränität (langfristig)

Um den Risiken entgegenzuwirken, die aus der Abhängigkeit von Nicht-EU-Herstellern und -Zulieferern erwachsen, empfehlen wir eine **erhebliche staatliche Förderung (auf EU-Ebene) von Forschung und Entwicklung für 5G-Komponenten**

(die möglichst unabhängig von Nicht-EU-Lieferanten sind). Dies wird in einigen kritischen Feldern, z.B. in der Luft- und Raumfahrt sowie der Wehrtechnik im Sinne einer Unabhängigkeit von ITAR-beschränkten Technologien, bereits praktiziert. Wir schätzen die Kosten für die Entwicklung alternativer Hardware-Komponenten auf einen Betrag im unteren zweistelligen Mrd-USD-Bereich. Beispielsweise würden unterschiedliche Chips in 7nm-Technologie benötigt[1]. Der Aufbau einer 7-nm-Fabrik in Europa würde sich auf etwa 10 Mrd USD belaufen[2]. Wir gehen von einer erforderlichen Entwicklungszeit von ca. fünf Jahren aus.

Eine »technologische Aufholjagd« ist machbar, sofern der politische Wille vorhanden ist und entsprechendes Fördervolumen zur Verfügung gestellt wird.

Aus einem solchen Projekt würden sich außerdem für europäische Firmen und Forschungseinrichtungen Möglichkeiten ergeben, für künftige Mobilfunksysteme eigene Intellectual Property (IP) in die aktuellen und künftigen Standards einzubringen. Angesichts der etwa 15-20 Prozent IP-Lizenzanteile des Herstellungspreises eines Smartphones würde sich dadurch für Deutschland und Europa, auch bei der technologischen Dominanz von nicht-europäischen Marktteilnehmern, eine Möglichkeit eröffnen, signifikante Wertschöpfung in Deutschland und Europa zu erzeugen. **Zusätzlich müssten erhebliche Mittel für die Einführung dieser neuen Technologien bereitgestellt werden.** Der britische Vodafone-Konzern[3] rechnet derzeit beispielsweise mit Kosten in Höhe von ca. 200 Mio Euro für den geplanten Austausch der Huawei-Hardware gegen Nokia-Geräte, sowie mit einer potenziellen Verzögerungen des 5G-Ausbaus von zwei bis fünf Jahren.

Neben der kontrollierten Hardware-Entwicklung (einschließlich der kontrollierten Fertigung aller Zulieferer-Komponenten) sollte **konsequenterweise auch der Software-Stack vollständig kontrolliert** werden. Derzeit verfolgen in den USA die Firmen Dell, Microsoft und AT&T Überlegungen[4], einen gemeinsamen 5G-Softwarestandard für Telekommunikationsnetze zu entwickeln, der auf Standard-Hardware zur Ausführung kommen kann. Die Realisierung ist aber noch völlig offen, zumal Huawei einen großen Teil des IPs besitzt und damit ein derartiges neues Produkt (nach Aussage von Huawei) ein bis zwei Jahre hinter vergleichbaren Huawei-Produkten zurückbleiben würde.

Um Alternativen zu bestehenden bzw. in der Entwicklung befindlichen Software-Stacks zu erhalten, empfehlen wir die **Unterstützung offener Schnittstellen**, die Open API Initiativen. Diese erlauben eine deutlich bessere Austauschbarkeit von Software-Komponenten. Zusätzlich empfehlen wir die Initiierung einer **Open 5G Partnership Initiative Europe**, in der europäische Unternehmen (Anwender, Betreiber, Integratoren, Hersteller) eine 5G-Referenzplattform auf der Basis verfügbarer Standards und Best Practices definieren. Weiterhin empfehlen wir die **Etablierung von Communities aus breit aufgestellten Industriekonsortien, die offene Software entwickeln und betreiben**. Damit ist es möglich, Abhängigkeiten von einzelnen Anbietern deutlich abzuschwächen. Durch die gemeinsame Entwicklung in einem offenen Umfeld können die erforderliche Transparenz herbeigeführt und der enorme Entwicklungsaufwand bewältigt werden. Für Start-ups bzw. KMUs eröffnen sich zudem attraktive Möglichkeiten für Beiträge zu einem offenen 5G-Ökosystem.

1 https://semiengineering.com/big-trouble-at-3nm/: Generally, IC design costs have jumped … to $297.8 million for a 7nm chip

2 https://venturebeat.com/2018/08/28/why-the-10-billion-chip-factory-club-just-got-smaller/

3 Siehe https://www.heise.de/newsticker/meldung/Vodafone-Austausch-von-Huawei-kostet-Millionen-4655846.html, 7.2.2020

4 https://windowsunited.de/huawei-usa-planen-alternative-5g-software/ 5.2. 2020

5.3 Fraunhofer-Angebote

Fraunhofer verfügt im Software- und im Hardware-Bereich über exzellente Expertisen sowie über Hardware-Sicherheitsanalyse-Labore mit Messplätzen und Analysemethoden auf höchstem Niveau.

Als neutraler Partner der deutschen und europäischen Industrie mit umfangreichem Know-how und exzellenten Laborausstattungen sowie mehreren Reallaboren ist Fraunhofer der ideale Partner zur Beratung und Unterstützung der Politik.

Fraunhofer bietet der Politik und Industrie eine Zusammenarbeit in den folgenden Punkten an:

- **Aufbau weiterer Labors zur Durchführung von Analysen**
- **Ausbildung von Fachpersonal**
- **Ausarbeitung von Prüfkriterien und Prüfmaßnahmen**
- **Lösungen zur Absicherung von Endgeräten (Trusted Connector-Technologie des Industrial Data Space IDS) sowie Weiterentwicklungen**
- **Weiterentwicklungen im Bereich des Radio-Access-Netzes und im Kernnetz**
- **Beratung, Planung, Aufbau und Betrieb von sicheren 5G-Campusnetzen**

Impressum

Herausgeber
Fraunhofer-Gesellschaft e.V.
Hansastraße 27c
80686 München

Redaktion
Roman Möhlmann, Fraunhofer-Gesellschaft e.V.
Dr. Beate Rauscher, Fraunhofer-Gesellschaft e.V.
Dr. Jan Weber, Fraunhofer-Gesellschaft e.V.

Autoren
Prof. Dr. Claudia Eckert, Fraunhofer AISEC
Prof. Dr. Thomas Magedanz, Fraunhofer FOKUS
Prof. Dr. Manfred Hauswirth, Fraunhofer FOKUS
Prof. Dr. Martin Schell, Fraunhofer HHI
Prof. Dr. Albert Heuberger, Fraunhofer IIS
Bernhard Niemann, Fraunhofer IIS
Dr. Haya Shulman, Fraunhofer SIT
Prof. Dr. Michael Waidner, Fraunhofer SIT

Bildquellen
Seite 5: Fraunhofer IPA / Rainer Bez
Seite 7: Die Campus-Lösung / Deutsche Telekom
Alle übrigen Abbildungen: iStock

Gestaltung
Ariane Lange, Fraunhofer-Gesellschaft e.V.