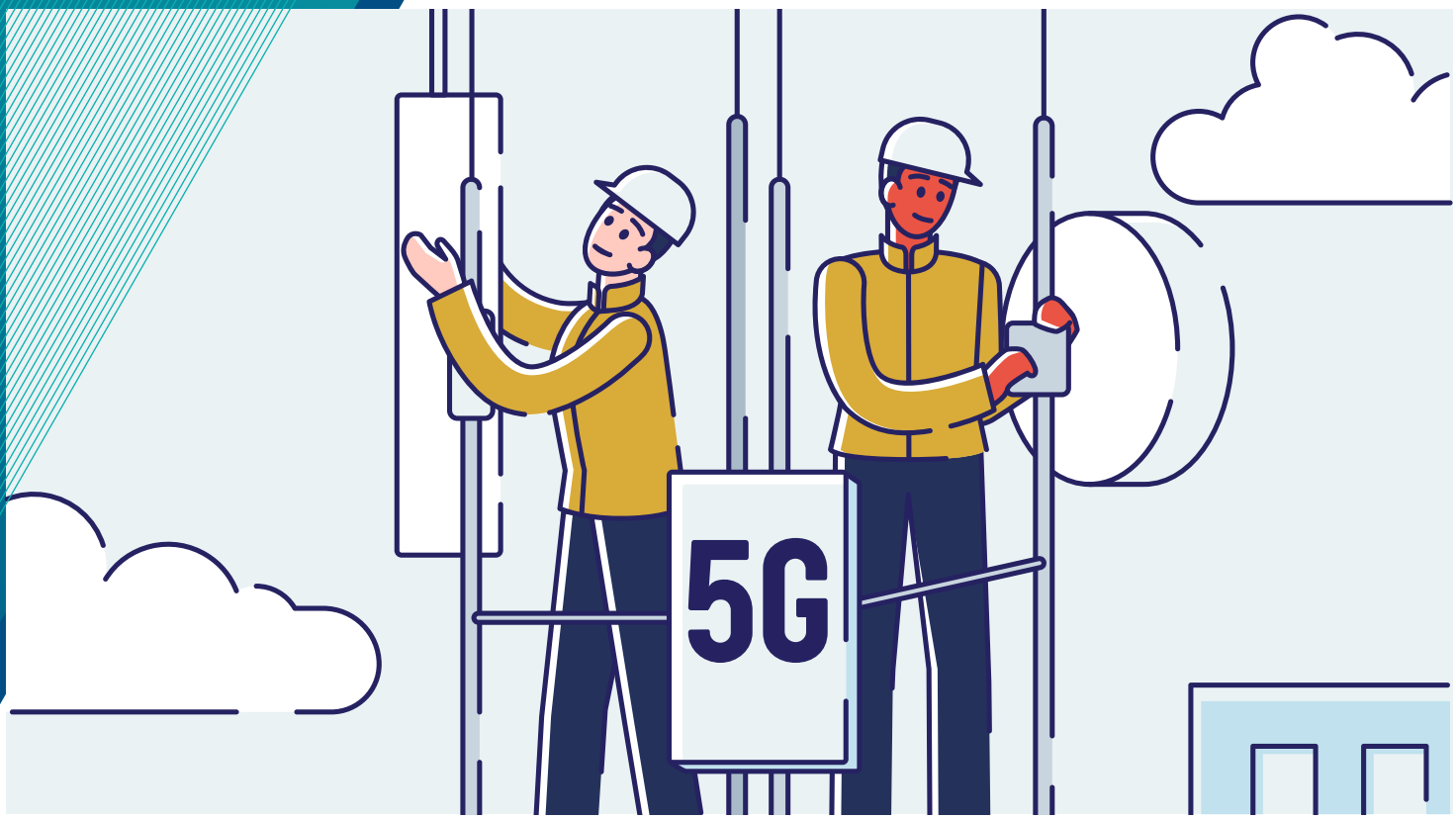
Nr. 397 / Juli 2020
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Die 5G-Debatte: Ein Test für die „digitale Souveränität“ Europas

Isabel Skierka

- Der Umgang mit Hochrisikozulieferern von Netzwerktechnologie beim Aufbau von vertrauenswürdigen 5G-Netzen stellt für Deutschland und Europa eine fundamentale strategische Herausforderung dar, die einheitlich durch Europa beantwortet werden sollte.
- Angesichts der Komplexität der Herausforderung sollte Deutschland eine Lösung anstreben, die sowohl technische wie politische Aspekte vereint. Die Stärkung digitaler Souveränität sollte ein übergeordnetes Ziel einer nationalen wie europäischen 5G-Strategie sein.
- Die Debatte in Deutschland begann erst spät und ist langwierig. Letztlich ist sie jedoch ein positives Beispiel für die demokratische Entscheidungsfindung in pluralistischen Systemen. Mit hoher Wahrscheinlichkeit wird sie einen Präzedenzfall für zukünftige Entscheidungen über den Umgang mit strategischen Technologien schaffen.
- Aufgrund des noch immer eher technologischen Ansatzes bei dem Umgang mit Sicherheitsrisiken in Deutschland ist zu erwarten, dass die 5G-Debatte in Deutschland noch lange nicht abgeschlossen ist und auch in den kommenden Wochen nichts an politischer Brisanz verlieren wird.

Inhaltsverzeichnis

Dieser Text erschien ursprünglich in der Persicope-Reihe, Ausgabe 3/2020, des Regionalprogramms Australien und Pazifik der Konrad-Adenauer-Stiftung. Mit der Periscope-Reihe möchte das Regionalprogramm durch die Betrachtung strategischer Themen aus verschiedenen Blickwinkeln einen Beitrag zu einem umfassenden Dialog und einer verstärkten Zusammenarbeit zwischen Australien und Europa insbesondere im Bereich neuer Sicherheitsherausforderungen leisten. Der nachfolgende Text ist inhaltlich aktualisiert.

Der 5G-Netzausbau als geopolitischer Test: Ausgangslage

Über ein Jahr lang debattieren die Mitgliedsstaaten der Europäischen Union (EU) bereits darüber, ob und wie sie die Beteiligung des chinesischen Technologiekonzerns Huawei an dem Ausbau ihrer 5G-Mobilfunknetze einschränken sollen. Begleitet wird die Debatte von stetem Druck der USA, den Netzwerkausrüster aufgrund von nationalen Sicherheitsbedenken aus europäischen Infrastrukturen auszuschließen. Aber auch zahlreiche Experten und europäische Sicherheitsbehörden warnen vor den Risiken einer Abhängigkeit von chinesischen Herstellern bei kritischen Infrastrukturen wie 5G. Die Gesetze Chinas erlauben es der dortigen Regierung, Unternehmen wie Huawei oder ZTE zur Zusammenarbeit mit nationalen Sicherheitsbehörden zu zwingen und so potenziell Spionage oder die Sabotage von kritischen Netzinfrastrukturen im Ausland zu ermöglichen. Abgesehen von den häufig betonten Risiken für die nationale Sicherheit bringt eine starke Abhängigkeit von den ausländischen Technologiegiganten auch erhebliche wirtschaftliche und industrielle Nachteile mit sich. Setzt Europa auf Huawei-Technologie in 5G-Netzen, würden europäische Konkurrenten wie Nokia und Ericsson wohl angesichts eines immer mächtigeren und mutmaßlich staatlich subventionierten[1] chinesischen Technologieriesen langfristig nur schwer überleben können.

COVID-19 verdeutlicht digitale Abhängigkeiten.

Die Covid-19-Pandemie hat die Risiken einer Abhängigkeit im Bereich kritischer digitaler Infrastrukturen, auf die wir in Zukunft mehr denn je angewiesen sein werden, noch schärfer ins Licht gerückt. Das setzt Europas Handelsbeziehungen zu China zusätzlichen Belastungen aus. Andererseits nimmt aber auch der politische und ökonomische Druck, die Mobilfunknetze der nächsten Generation zeitnah, kosteneffizient und flächendeckend auszubauen, zu. Ein solcher Aufbau ist dabei insofern bedeutend, als dass sich mit der nächsten Mobilfunkgeneration enorme wirtschaftliche Innovationspotenziale verbinden, welche für den Erhalt der Wettbewerbsfähigkeit der europäischen Wirtschaft von entscheidender Bedeutung sein werden. Vor diesem Hintergrund spricht für Huawei nicht nur, dass es Telekommunikationsbetreibern seine Technologien zu günstigeren Preisen als seine europäischen Konkurrenten anbietet, sondern bis vor kurzem auch die entsprechenden Produktionskapazitäten für einen Aufbau vorzuweisen schien.[2]

5G als geopolitischer Test

Die EU steht somit, gefangen zwischen ihren beiden wichtigsten Handelspartnern, den USA und China, vor einem geopolitischen Test auf mehreren Ebenen. Wird Europa langfristig in der Lage sein, die Sicherheit und Zuverlässigkeit digitaler Infrastrukturen von zentraler Bedeutung für Wirtschaft und Gesellschaft zu gewährleisten? Wird es bei 5G und der damit verbundenen nächsten Welle der Industrialisierung tonangebend sein oder weiter an Innovationskraft verlieren? Wie sollen die EU-Mitgliedsstaaten mit der Abhängigkeit von ausländischen Technologien umgehen und jene „digitale Souveränität" erreichen, die eine der politischen Prioritäten der EU-Kommission unter Ursula von der Leyen ist? Insbesondere die Stärkung digitaler Souveränität könnte die wichtigste strategische Herausforderung sein, der sich die EU langfristig stellen muss – vor allem im Kontext des sich intensivierenden Handelskonflikts zwischen den USA und China und einer drohenden „Entkopplung" technologischer Lieferketten.

Eine „Toolbox" für Europas Mittelweg

Politische und regulatorische Maßnahmen notwendig

Das Problem ist mit dem einfachen Ausschluss der Technologie eines spezifischen Anbieters aus den 5G-Netzen nicht gelöst. Auf eine einfache Entweder-Oder-Lösung hat sich die EU daher nicht beschränkt. Nach einem langen Koordinierungsprozess haben sich die EU-Mitglieder nun auf ein einheitliches Verfahren für den Umgang mit den Sicherheitsrisiken in 5G-Netzen verständigt: Im Januar 2020 verabschiedete die Network Information Security (NIS) – Kooperationsgruppe, bestehend aus Vertretern der EU-Mitgliedsstaaten, der Europäischen Kommission und der EU-Cybersicherheitsagentur ENISA, die „5G Cybersecurity Toolbox".[3] Sie baut auf einer umfassenden, im Oktober 2019 verabschiedeten EU-Risikobewertung[4] auf und schafft eine Grundlage für einen koordinierten europäischen Ansatz für vertrauenswürdige 5G-Netze. Zwar sieht die Toolbox keinen Ausschluss spezifischer Anbieter vor. Sie zeigt jedoch technische und strategische Maßnahmen zur Minderung von Sicherheitsrisiken sowie von kritischen Abhängigkeiten in 5G-Netzen auf. Die Toolbox macht deutlich, dass strategische Risiken – insbesondere das „Risiko der Einmischung durch ein Drittland oder Abhängigkeitsrisiken" – nicht mit rein technischen Maßnahmen bewältigt werden können, sondern politische oder regulatorische Maßnahmen erfordern.

Ohne den Namen Huawei explizit zu nennen, hebt das EU-Dokument hervor, dass bei dem Aufbau von 5G-Netzen der Rückgriff auf Technologie „risikoreicher" Zulieferer eingeschränkt oder aus kritischen Teilen des Netzes ausgeschlossen werden sollte. Wie auch schon die Risikobewertung feststellt, können kritische Teile der 5G-Netzwerkinfrastruktur dabei sowohl Kernnetz- wie auch Zugangsnetzfunktionen umfassen. Außerdem sollen Mitgliedsstaaten sicherstellen, dass Netzbetreiber eine problematische Abhängigkeit von einem einzigen Anbieter oder mehreren Anbietern mit ähnlichem Risikoprofil vermeiden oder zumindest begrenzen. Dies soll insofern zu vertrauenswürdigen Netzen beitragen, da Diversität von Herstellern von 5G-Netz-Komponenten die Redundanz von Netzwerktechnik und damit die Resilienz von Netzen, beispielsweise im Fall von Ausfällen und Sabotage, erhöht. Zudem soll die EU-Kommission mit den Mitgliedsstaaten regulatorische und politische Maßnahmen ergreifen, um 5G-Lieferketten langfristig zu diversifizieren, stärker „zu europäisieren" und damit letztlich einen Beitrag zur digitalen Souveränität Europas zu leisten. Darunter fallen beispielsweise Maßnahmen für ein verbessertes Investment-Screening, Beschaffungsregularien, Anti-Dumping-Regeln oder Maßnahmen zur Förderung von Forschung und Entwicklung in Europa.

Mitgliedsstaaten entscheiden

Auf Grundlage der Toolbox werden die EU-Mitgliedsstaaten nun über den Umgang mit 5G-Sicherheitsrisiken und potenziellen Abhängigkeiten von chinesischen Lieferanten in ihren Telekommunikationsnetzen entscheiden müssen. Über den konkreten Umgang mit den Restrisiken und die Zulassung oder den Ausschluss von Netzwerkausrüstung spezifischer

Hersteller bestimmen die Mitgliedsstaaten selbst. Bis zum Sommer soll die NIS-Kooperationsgruppe die Maßnahmen jedes Mitgliedslandes auswerten.

Entscheidungen im handelspolitischen Spannungsfeld

Jüngste Entwicklungen im Handelsstreit zwischen den USA und China könnten jedoch bis dahin getroffene Entscheidung über den Einsatz von chinesischer Netzwerktechnik massiv beeinträchtigen. Mitte Mai haben die USA neue Exportbeschränkungen verhängt, die gezielt Huaweis Chip-Hauptlieferant, den taiwanesische Konzern TSMC, betreffen.[5] Mit den neuen Exportbeschränkungen soll seitens der USA de facto verhindert werden, dass Huawei weiterhin Zugang zu hochentwickelten Halbleitern erhält, auf die es für die Entwicklung und vor allem Produktion seiner Netzwerkkomponenten zwingend angewiesen ist. Wenn die USA die Kontrollen tatsächlich wie geplant implementieren, könnte Huawei in ernsthafte Lieferengpässe geraten. Selbst für Länder, die sich für einen Einsatz von Huaweis Netzwerktechnik entschieden haben, könnte so zum einen das Risiko entstehen, dass Huawei Lieferverpflichtungen nicht mehr nachkommen kann oder sich Lieferzeiten in Zukunft erheblich verlängern. Zum anderen befürchten Experten in Großbritannien, dass sich durch eine grundlegende Veränderung der Zulieferkette das Risikoprofil von Huawei negativ verändert.[6]

Keine einheitliche europäische Position

Momentan gibt Europa hinsichtlich des Umgangs mit Risiken der nationalen Sicherheit und Abhängigkeiten noch ein gespaltenes Bild ab. Einige Länder wie Belgien, Estland, Frankreich, Italien, Polen oder die Tschechische Republik haben den Zugang von „risikoreichen" Herstellern wie Huawei zum 5G-Netz eingeschränkt oder entsprechende Gesetze erlassen, die Vetorechte der Sicherheitsbehörden und strengere Überprüfungen zulassen. Andere EU-Mitglieder sind noch zögerlich und lassen chinesischen Herstellern wie Huawei bislang noch größeren Spielraum. Dazu gehörte neben Ländern wie Spanien, Portugal oder Finnland bisher auch Großbritannien. Dort zeichnet sich jedoch nun, unter Druck der USA, eine Kehrtwende in Richtung einer restriktiveren Handhabung chinesischer Lieferanten ab.[7]

Noch kein Ende in Sicht: die deutsche Debatte

Als größte Volkswirtschaft Europas und das Land mit dem größten Telekommunikationsmarkt wird Deutschland mit einer Entscheidung zu Fragen der 5G-Sicherheit zweifelsohne ein wichtiges Signal an andere noch unentschiedene EU-Mitglieder senden. Bislang tut sich die Bundesregierung jedoch schwer mit einer Einigung auf eine gemeinsame politische Position. Wenngleich die Einbeziehung von Huawei in den Aufbau von 5G-Netzen erhebliche politische und wirtschaftliche Risiken birgt, hat die deutsche Industrie potenziell viel zu verlieren. Ein Ausschluss von Huawei aus dem Netz könnte zu Vergeltungsmaßnahmen Pekings gegen deutsche, auf dem chinesischen Markt stark engagierte Firmen wie Volkswagen, Siemens oder BASF führen. Chinesische Diplomaten und auch der chinesische Botschafter in Deutschland haben diese Möglichkeit bereits ins Spiel gebracht.[8] Daher hatte, Medienberichten zufolge, die deutsche Bundeskanzlerin letztes Jahr selbst interveniert, um Restriktionen gegen chinesische Anbieter zu verhindern.[9] Darüber hinaus führen Wirtschaftsvertreter immer wieder an, dass ein zeitnaher Aufbau von 5G-Netzen in Deutschland entscheidend sei, wenn Deutschland eine führende Position im Bereich der Industrie 4.0 einnehmen und ein prägender 5G-Leitmarkt werden will. Auch heute noch bleiben das Kanzleramt und das Bundeswirtschaftsministerium auf einem China-freundlicheren Kurs als andere Teile der Regierung, insbesondere das Auswärtige Amt.

Ursprünglich verfolgte die Regierung einen rein technologie-basierten Ansatz für die Beurteilung von 5G-Sicherheitsrisiken. Dieser hätte auf Quellcode-Prüfungen, Zertifizierungen und Vertrauenswürdigkeitserklärungen[10] von Herstellern gesetzt.[11] Die Unternehmensstruktur des Technologieanbieters und der Kontext des politischen und rechtlichen Umfelds, in dem es tätig ist – Schlüsselaspekte, auf die auch die EU-Risikobewertung explizit hinweist – hätten so nicht geprüft werden müssen. Doch der Versuch, ein Problem solch hoher geopolitischer Relevanz mit technokratischen Mitteln zu lösen, provozierte Widerstand im Bundestag und in der Regierung selbst. Die SPD-Fraktion, Teile der Opposition und auch einige Abgeordnete der CDU-Fraktion pochten auf strengere Kriterien zur Überprüfung von Herstellern, die nicht nur technische, sondern auch strategische politische und wirtschaftliche Aspekte mit einbeziehen würde.

Ein zu technischer Ansatz stößt auf Widerstand.

Bürokratisierung statt politischer Lösungen

Mit dem neuen Entwurf des *Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* („IT-Sicherheitsgesetz 2.0“) vom Mai 2020 plant das Bundesinnenministerium nun, den Streit über die Beteiligung Huaweis am 5G-Netzausbau beizulegen.[12] In der Begründung des Gesetzesentwurfs räumt das Ministerium ein, dass „weder eine Komponentenzertifizierung, noch eine Überprüfung von Sicherheitskonzepten … eine 100%ige Sicherheit dahingehend [bieten], dass die Hersteller keine missbräuchlichen Zugriffsmöglichkeiten auf Hard- und Software implementieren, die Sabotage oder Spionage ermöglichen“.[13] Gemäß des geplanten § 9b BSIG (BSI-Gesetz) im Referentenentwurf müssen Hersteller kritischer Netzwerkkomponenten, für die eine Zertifizierungspflicht besteht (worunter Telekommunikations-Netzwerkkomponenten fallen werden)[14], gegenüber dem Betreiber der kritischen Infrastruktur eine Garantieerklärung über die Vertrauenswürdigkeit ihrer Komponenten abgeben, die sich über die gesamte Lieferkette des Herstellers erstrecken soll. Ist der Hersteller nicht vertrauenswürdig, da er beispielsweise die in der Garantieerklärung eingegangenen Verpflichtungen verletzt oder die Komponente vorsätzliche Schwachstellen enthält,[15] kann das Innenministerium den Einsatz der Komponenten untersagen. Dass Huawei jedoch Vertrauenswürdigkeitserklärungen bereitwillig unterschreiben wird, hat CEO Ren Zhengfei bereits 2019 beteuert.[16]

Vertrauenswürdigkeit als Faktor

Trotz der Aussage, dass rein technische Mechanismen das Problem der Vertrauenswürdigkeit nicht lösen können, setzen die vorgeschlagenen gesetzlichen Vorschriften weiterhin überwiegend auf technische Prüfungen der IT-Sicherheit. Dieser Ansatz trägt eher zu einer Bürokratisierung der 5G-Entscheidung denn zu einer politischen Lösung bei.[17] Skeptiker im Bundestag und in der Regierung, einschließlich des Auswärtigen Amts, wird dieser Ansatz voraussichtlich nicht überzeugen, weshalb die Debatte wohl noch länger andauern wird als bis zum Herbst 2020, für den die Verabschiedung des IT-Sicherheitsgesetzes 2.0 geplant ist.

Ein möglicher Lösungsansatz wäre der Zusatz einer politischen Bewertung der Vertrauenswürdigkeit von Herstellern unter Einbeziehung der strategischen Risiken, auf die die EU-Risikobewertung und die Toolbox verweisen. Diese Bewertung könnte beispielsweise durch den Bundessicherheitsrat (BSR) oder ein ähnlich aufgebautes Gremium vorgenommen werden. Der BSR ist ein geheim tagender Ausschuss des Bundeskabinetts, der über die Genehmigung von Rüstungsexporten entscheidet. Dieses Modell ließe sich auf Entscheidungen über den Einbau von Netzwerkkomponenten übertragen und wird offen von SPD-Abgeordneten befürwortet.[18] Deutschland könnte damit dem Beispiel der EU-Mitglieder Frankreich und Italien folgen. Diese haben Minister ihrer Regierung bzw. Sicherheitsbehörden mit der Befugnis ausgestattet, die Pläne von Netzbetreibern zur Einführung von 5G-Technik vor dem Hintergrund nationaler Sicherheitsinteressen zu prüfen und über deren Genehmigung zu entscheiden.[19] Eine weitere

Bundessicherheitsrat, Innenminister oder Europa – Drei Lösungsvorschläge

von Experten vorgeschlagene Option ist ein Verfahren, nach dem die EU feststellt, ob ein Drittstaat, beispielsweise China, ein angemessenes Schutzniveau für die Vertrauenswürdigkeit von Komponenten gewährleistet. In diesem Verfahren könnte die EU ähnlichen Regeln wie jenen der europäischen Datenschutzgrundverordnung folgen und ein entsprechendes Abkommen mit dem Drittstaat schließen.[20]

Unterdessen stehen Telekommunikationsanbieter unter Handlungsdruck, ihre Netze zu modernisieren. Telefonica, Deutsche Telekom und Vodafone betonen, in ihren 5G-Kernnetzen keine Huawei-Technik zu nutzen und stattdessen auf Ericsson und Nokia zu setzen. Für das Zugangsnetz ist jedoch weiter die teilweise Verwendung von Huawei-Technik geplant. Ein wichtiger Grund dafür ist, dass die Betreiber zunächst ihre bestehenden 4G-Netze auf ein „non-standalone"-5G-Netz aufrüsten. Dies bedeutet, dass für den Aufbau von 5G-Netzen keine völlig neue Mobilfunkinfrastruktur aufgebaut wird, sondern die bereits bestehende Mobilfunk-Netzstruktur ein Upgrade erhält und nur wo es nötig ist, erweitert wird. Insbesondere im heutigen 4G-Zugangsnetz ist bei allen Betreibern noch viel Huawei-Technik verbaut, die wenn überhaupt erst über die Zeit sukzessive ersetzt werden würde.[21]

Beispielhafte Diskussion

Unabhängig vom Ausgang der deutschen Debatte steht sie als Beispiel dafür, wie Entscheidungen über den Einsatz strategischer Technologien von Legislative und Exekutive offen und demokratisch debattiert werden können – auch wenn das Bewusstsein für die Tragweite dieser Entscheidungen in Deutschland erst spät aufkam.

Über 5G hinaus: Digitale Souveränität in Europa

Obwohl sich die Debatte um die Sicherheit von 5G-Netzen oberflächlich hauptsächlich um Cybersicherheit und nationale Sicherheit dreht, ist ihre wohl wichtigste strategische Dimension in Europa die der „digitalen Souveränität". Digitale Souveränität bedeutet in demokratischen Staaten allgemein die Fähigkeit eines Akteurs (eines Staates, eines Unternehmens oder eines Individuums), im digitalen Raum selbstbestimmt zu handeln und entscheiden zu können.[22] Grundlage der digitalen Souveränität ist die Beherrschung von Schlüsselkompetenzen und -technologien sowie die Fähigkeit, zwischen Alternativen vertrauenswürdiger Partner entscheiden zu können und diese gegebenenfalls weiterzuentwickeln.[23] In diesem Zusammenhang ist Souveränität nicht gleichbedeutend mit Autarkie. Sie besteht vielmehr gerade in der Fähigkeit, Abhängigkeiten einzugehen und die Technologien und Fähigkeiten durch ausreichende Beurteilungs- und Handlungsfähigkeit zu kontrollieren und (in gewissem Maße) beherrschen zu können.

Europäische Lessons Learned

Wie kann Europa also seine „digitale Souveränität stärken" und damit ein von der Europäischen Kommission proklamiertes strategisches Ziel erfüllen?[24] Da die EU-Mitgliedsstaaten zunehmend von auswärtigen/Nicht-EU-Technologielieferanten abhängig sind – insbesondere in den Bereichen Cloud, Dateninfrastruktur und Software bzw. bei mobilen oder Desktop-Betriebssystemen, aber auch bei Halbleitern und Mikroprozessoren – wird dies keine leichte Aufgabe sein. Ironischerweise ist eines der wenigen Technologiefelder, in denen europäische Unternehmen derzeit noch führend sind, die Herstellung von Mobilfunktechnologie. Zwei der drei Marktführer im Bereich der Funkzugangsnetze (Radio Access Network) – Ericsson und Nokia – sind europäische Unternehmen und Konkurrenten von Huawei. Folglich sollte im Rahmen der 5G-Debatte ein erster Schritt darin bestehen, die Position der europäischen Hersteller gegenüber chinesischen Konkurrenten zu stärken. Dabei geht es nicht um protektionistische Maßnahmen gegenüber chinesischen Technologieunternehmen als vielmehr um das Ziel auf dem europäischen Markt gleiche und faire Wettbewerbsbedingungen, ein sog. „level playing field", zu garantieren. Dies erfordert nicht nur Sicherheits-

richtlinien, sondern langfristig auch Maßnahmen im wettbewerbsrechtlichen und industriepolitischen Bereich, wie sie die „5G Cybersecurity Toolbox" der EU ebenfalls empfiehlt.

Doch wie der aktuelle Konflikt um Halbleiter-Lieferketten zeigt, stellt sich schon jetzt die Frage, wie viel Europa in geopolitischen Rivalitäten um die Kontrolle über strategische Technologien noch mitreden kann. Um die Fähigkeit der Mitgliedsstaaten zum selbstbestimmten Handeln im digitalen Raum allgemein und über 5G hinaus zu verbessern, muss die EU ihre eigene industrielle Basis in wichtigen Technologiesektoren stärken und auf die nötigen gegenseitigen Abhängigkeiten in einer von der Globalisierung von Lieferketten gekennzeichneten Welt strategisch eingehen. Statt Abhängigkeiten durch Entkopplung aufzulösen, sollte Europa versuchen mit Hilfe von kompetenter Diplomatie, Handelsinstrumenten und einer gezielten Stärkung eigener Kompetenzen diese klug zu managen.

Erste Schritte hin zu mehr Handlungsfähigkeit im digitalen Raum

Definition von Prioritäten

In einem ersten Schritt sollten die Entscheidungsträger in Europa daher bestimmen, über welche Schlüsseltechnologien und Kompetenzen sie selbst verfügen sollten und in welchen Bereichen sie Abhängigkeiten eingehen können. Damit muss eine Strategie für den Umgang mit der Abhängigkeit von ausländischen Technologieanbietern einhergehen, die sich zwangsläufig aus den heutzutage globalisierten Wertschöpfungsketten ergibt. Fragen, die hierbei beantwortet werden müssen sind vor allem: Mit welchen Partnern können und sollen die EU-Mitgliedsstaaten im Technologiebereich langfristig und vertrauensvoll zusammenarbeiten und welcher Rahmen muss für eine solche Kooperation gegeben sein? Eine besondere Rolle sollten dabei die Vertrauenswürdigkeit und Offenheit des politischen Systems des Kooperationspartners, dessen Rechtsordnung sowie die bisherigen Erfahrungen mit jenem Kooperationspartner innerhalb von politischen und ökonomischen Bündnissen spielen.

Darüber hinaus sollten die Regierungen Innovationen aktiv fördern und die digitale Transformation der vorhandenen industrielle Basis über die Anwendung zentraler Schlüsseltechnologien – wie Robotik, künstliche Intelligenz (Talente und Technologien) und *Edge Computing* – stärken. EU-Mitglieder sollten in Forschung und Entwicklung sowie in angewandte innovative Projekte investieren (auch in Kooperation mit dem privatwirtschaftlichen Sektor) und ihre Rolle als Nutzer und Käufer wirksam zur Förderung ausgewählter Technologien nutzen. Zusätzlich sollten die Staaten ein hohes Maß an Rechtssicherheit für den Einsatz neuer Innovationen sicherstellen. Dies hat die Union bereits mit dem Programm „Important Projects of Common European Interest" (IPCEI) im Bereich der Mikroelektronik, oder mit dem Projekt des „Europäischen Netzwerks von Kompetenzzentren für Cybersicherheit" im Rahmen des Förderprogramms „Horizon 2020" begonnen.[25] Um Transparenz und Kontrolle der Informationstechnologie zu gewährleisten, aber auch Innovationsmöglichkeiten zu stärken, könnten die Gesetzgeber auf EU-Ebene Hersteller und Anbieter zur Öffnung von Technologien und größerer Interoperabilität verpflichten. EU-Mitgliedsstaaten sollten außerdem wettbewerbsrechtliche und andere Instrumente prüfen und stärken, die das sog. „level playing field" auf dem europäischen Markt garantieren können.

International wird Europa für alle Beteiligten faire Rahmenbedingungen durch die Anpassung der Regularien für Handel, ausländische Direktinvestitionen und Beschaffung herstellen müssen. Unter Wahrung der Grundsätze einer offenen und wettbewerbsfähigen europäischen Wirtschaft wird die EU zudem kaum umhin kommen, die Prüfung staatlicher Beihilfen auf Unternehmen mit Firmensitz außerhalb der EU auszuweiten und europäische Unternehmen mit Investitionsmitteln – sowohl für Forschung und Entwicklung als auch im

Bereich der Umsetzung – zu unterstützen und ihr Instrumentarium zur Kontrolle ausländischer Direktinvestitionen zu stärken. Mit letzterem hat die EU bereits mit der „Foreign Direct Investment Screening Regulation" vom Oktober 2019 begonnen.[26]

Wenn Europa die Fähigkeit bewahren will, seine digitale Zukunft in wesentlichen Teilen selbst zu gestalten, sind dies notwendige Schritte, die in naher Zukunft zu gehen sind. Eine langfristige Selbstbehauptung im Feld digitaler Schlüsseltechnologien und deren Anwendung wird zu einem der strategisch wichtigsten Güter Europas werden und die Voraussetzung für den Erhalt seines politischen und wirtschaftlichen Einflusses in der Zukunft sein.

1 Vgl. Ellen Nakashima, „U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", 29. Mai 2019, *The Washington Post*, abgerufen am 05.06.2020 unter: https://www.washingtonpost.com/world/ national-security/for-huawei-the-5g-play-is-in-europe-and-the-us-is-pushing-hard-for-a- ban-there/2019/05/28/582a8ff6-78d4-11e9- b7ae-390de4259661_story.html
Chuin-Wei Yap, „State Support Helped Fuel Huawei's Global Rise", 25.12.2019, *The Wall Street Journal,* abgerufen am 05.06.2020 unter: https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

2 Lindsay Maizland und Andrew Chatzky, „Huawei: China's Controversial Tech Giant", 12.02.2020, Council on Foreign Relations, abgerufen am 05.06.2020 unter: https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant;
Für Debatte dieser Argumente siehe: Elsa B. Kania, Lindsey R. Sheppard, „Why Huawei Isn't So Scary", 12.10.2019, *Foreign Policy*, abgerufen am 05.06.2020 unter: https://foreignpolicy.com/2019/10/12/huawei-china-5g-race-technology/;
Morris Lore, „Huawei's '18-month lead' in 5G is telecom's most spurious claim", 09.03.2020, *LightReading*, abgerufen am 05.06.2020 unter: https://www.lightreading.com/5g/huaweis-18-month-lead-in-5g-is-telecoms-most-spurious-claim/a/d-id/758064.

3 EU NIS Cooperation Group, „Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures", Januar 2020, Brüssel.
Siehe hierzu auch Sebastian Weise, „Brüssels 5G-Toolbox kurz erklärt", 04.02.2020, Konrad-Adenauer-Stiftung, abgerufen am 08.06.2020 unter: https://www.kas.de/de/kurzum/detail/-/content/bruessels-5g-toolbox-kurz-erklaert.

4 EU NIS Cooperation Group, „EU coordinated risk assessment of the cybersecurity of 5G networks", 09.10.2019, Brüssel, abgerufen am 05.06.2020 unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

5 Vgl. Kathrin Tai, „Angriff mit dem Skalpell", *Zeit Online*, 27.05.2020, abgerufen am 05.06.2020 unter https://www.zeit.de/2020/23/huawei-usa-china-sanktionen-handelskonflikt-smartphones-halbleiter/komplettansicht;
Jan-Peter Kleinhans, „TSMC prepares for US-China chips decoupling", Technode, 27.05.2020, abgerufen am 05.06.2020 unter https://technode.com/2020/05/27/tsmc-prepares-for-us-china-chips-decoupling/.

6 Vgl. Warrel, H. / Fiildes, N., 2020, „UK review of Huawei eyes impact of US sanctions" abgerufen am 05.06.2020 unter https://www.ft.com/content/9e581ace-69ec-4a42-81c3-c28d2bb40aa1.

7 M. Schwarten, „Großbritannien will Huawei doch vom 5G-Ausbau ausschließen", 25.05.2020, 5G-Anbieter.info, abgerufen am 05.06.2020 unter https://www.5g-anbieter.info/5g-news/grossbritannien-will-huawei-doch-vom-5g-ausbau-ausschliessen.
Dieter Petereit, „Kein Huawei-5G in Großbritannein: Johnson vollzieht Kehrtwende", *t3n*, abgerufen am 05.06.2020 unter https://t3n.de/news/kein-huawei-5g-grossbritannien-1283540/.

8 Stefan Wurzel, „Drohungen gegen deutsche Firmen in China", Tagesschau, 05.01.2020, abgerufen am 05.06.2020 unter: https://www.tagesschau.de/wirtschaft/huawei-china-streit-101.html;
Noah Barkin, „Europe's Backlash Against Huawei Has Arrived", *Foreign Policy*, 27.11.2019, abgerufen am 05.06.2020 unter: https://foreignpolicy.com/2019/11/27/europe-huawei-back-lash-merkel-germany-summit/.

9 Moritz Koch, Dietmar Neuerer, Stephan Scheuer, „Merkel öffnet 5G-Netz für Huawei", 14.10.2019, *Handelsblatt*, abgerufen am 05.06.2020 unter: https://www.handelsblatt.com/politik/deutschland/netzausbau-merkel-oeffnet-5g-netz-fuer-huawei/25107766.html.

10 Dies läuft auf eine „No-Spy"-Klausel zwischen Anbieter und Netzbetreiber hinaus. In dieser Klausel müssten die Anbieter versichern, dass sie rechtlich und wirksam in der Lage sind, die Offenlegung vertraulicher Kundeninformationen gegenüber Dritten abzulehnen. Dem Mechanismus fehlten jedoch Verifizierungs-, Durchsetzungs- oder Bewertungsmechanismen.

11 Bundesnetzagentur, „Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten nach § 109 Telekommunikationsgesetz – Stand 09.10.2019“, 9.10. 2019, abgerufen am 05.06.2020 unter: https://www. bundesnetzagentur. de/SharedDocs/Down- loads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderun- gen2.pdf?__blob=publicationFile&v=2.

12 Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat, „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, Stand 07.05.2020, 17:13 Uhr, abgerufen am 05.06.2020 unter http://intrapol.org/wp-content/uploads/2020/05/200507_BMI_RefE_IT-SiG20.pdf.

13 Ibid., S. 58 f.

14 Mit einer weiteren Änderung des § 109 Abs. 2 TKG (Telekommunikationsgesetz) erlässt der Entwurf für ein IT-Sicherheitsgesetz 2.0 eine Zertifizierungspflicht für kritische Komponenten in öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten. Daher bezöge sich dieser Absatz auch auf 5G-Netzkomponenten.

15 Weitere Kriterien listet § 9b Abs. 4 BSIG RefE auf

16 Dana Heide, Moritz Koch, Kerstin Leitel und Torsten Riecke, „Huawei will jede Vertrauenswüridgkeitserklärung unterschreiben – Berlin bleibt skeptisch“, 13.05.2019, *Handelsblatt*, abgerufen am 05.06.2020 unter: https://www.handelsblatt.com/politik/international/5g-ausbau-huawei-will-jede-vertrauenswuerdigkeitserklaerung-unterschreiben-berlin-bleibt-skeptisch/24336204.html.

17 Martin Schallbruch, „Wir werden noch lange über Huawei streiten”, 18.05.2020, Interview mit Paul Dalg, *Tagesspiegel Background Digitalisierung & KI*.

18 Björn Finke, Georg Mascolo und Alexander Mühlauer, „Warum Huawei die Politik so sehr spaltet“, 29.01.2020, *Süddeutsche Zeitung*, abgerufen am 05.06.2020 unter https://www.sueddeutsche.de/wirtschaft/huawei-5g-netz-ausbau-deutschland-1.4776270.
Philipp Grüll, „Entwurf für 5G-Sicherheitskriterien: SPD sieht ‚stumpfes Schwert‘“, 13.05.2020, Euractiv, abgerufen am 05.06.2020 unter https://www.euractiv.de/section/europakompakt/news/entwurf-fuer-5g-sicherheitskriterien-spd-sieht-stumpfes-schwert/.

19 Wei Shi, „French parliament passes “Huawei Law” to govern 5G security”, 26.07.2019, tele-coms.com, abgerufen am 05.06.2020 unter: https://telecoms.com/498728/french-parliament-passes-huawei-law-to-govern-5g-security/; Reuters, „Italy approves use of special powers over 5G supply deals”, 05.09.2019, Reuters, abgerufen am 05.06.2020 unter: https://www.reuters.com/article/us-huawei-tech-5g-italy/italy-approves-use-of-special-powers-over-5g-supply-deals-idUSKCN1VQ1YG.

20 Vorschlag von Martin Schallbruch, „Wir werden noch lange über Huawei streiten”, 18.05.2020, Interview mit Paul Dalg, *Tagesspiegel Background Digitalisierung & KI.*

21 Helmut Martin-Jung, „Raus aus dem Kern“, 02.06.2020, *Süddeutsche Zeitung*, abgerufen am 05.06.2020 unter: https://www.sueddeutsche.de/wirtschaft/5g-netz-raus-aus-dem-kern-1.4924635;
Morris Lore, „Goodbye Huawei, hello Ericsson: Swap-out gathers pace”, 03.06.2020, *LightReading*, abgerufen von: https://www.lightreading.com/5g/goodbye-huawei-hello-ericsson-swap-out-gathers-pace/a/d-id/761438.

22 Dieser Abschnitt basiert auf Teilen von: Isabel Skierka, „Stellungnahme zur Anhörung des Ausschusses Digitale Agenda zum Thema ‚IT-Sicherheit von Hard- und Software als Voraussetzung für Digitale Souveränität“, 11.12.2019, Deutscher Bundestag, abgerufen am 05.06.2020 unter https://www.bundestag.de/resource/blob/672536/b2b63aeeaffe54e40f8c62571cc628c4/Stellungnahme-Skierka-data.pdf.

23 Bitkom, „Digitale Souveränität, Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa“, 2015; Forschungszentrum Informatik, Accenture, Bitkom Research, „Kompetenzen für eine Digitale Souveränität“, 2015.

24 Europäische Kommission, „The von der Leyen Commission: for a Union that strives for more”, 10.09.2019, Brüssel, abgerufen am 05.06.2020 unter: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542. Manchmal wird anstatt des Begriffs „digitale Souveränität” auch „digitale strategische Autonomie” verwendet.

25 Siehe auch: European Political Strategy Centre of the European Commission, „Rethinking Strategic Autonomy in the Digital Age”, *EPSC Strategic Notes*, Juli 2019, Heft 30. Abgerufen am 05.06.2020 unter: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strate- gic_note_issue30_strategic_autonomy.pdf.

26 Mark Leonard, Jean Pisani-Ferry, Elina Ribakova, Jeremy Shapiro und Guntram Wolff, „Redefining Europe’s Economic Sovereignty”, Juni 2019, European Council on Foreign Relations. abgerufen am 05.06.2020 unter: https://www.ecfr.eu/publications/summary/redefining_europes_economic_sovereignty;
Siehe auch: EU NIS Cooperation Group, „Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures”, Januar 2020, S. 7 ff.

Impressum

Die Autorin

Isabel Skierka ist Forscherin am Digital Society Institute der ESMT Berlin, non-resident Fellow am Global Public Policy Institute in Berlin und promoviert an der Tallinn University of Technology in Estland.

Konrad-Adenauer-Stiftung e. V.

Sebastian Weise
Referent Innovationen
Analyse und Beratung
T: +49 30 / 26 996-3732
sebastian.weise@kas.de

Johannes Wiggen
Referent Cybersicherheit
Analyse und Beratung
T: +49 30 / 26 996-3934
johannes.wiggen@kas.de

Postanschrift: Konrad-Adenauer-Stiftung e. V., 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2020, Berlin
Gestaltung: yellow too Pasiek Horntrich GbR
Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.
Druck: copy print Kopie & Druck GmbH, Berlin
Printed in Germany.
Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-95721-712-7