Standpunkt zivile Sicherheit

Versteckte Kosten nicht-vertrauenswürdiger Anbieter in 5G-Netzwerken

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Stuchtey, Dörr, Frumento, Oliveira,
Panza, Rausch, Rieckmann, Yaich

Nummer 12 · Dezember 2020

IMPRESSUM

Die Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gGmbH ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht.

Das Institut publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Das BIGS entstand im Frühjahr 2010 in Potsdam unter der Beteiligung der Universität Potsdam und ihrer UP Transfer GmbH sowie der Unternehmen IABG, Rolls-Royce und seit 2018 W.I.S..

Diese Studie wurde durch einen Zuschuss des U.S. Department of State finanziert. Die hierin geäußerten Meinungen, Erkenntnisse und Schlussfolgerungen sind die der Autoren und spiegeln nicht notwendigerweise die des U.S. Department of State wider.

Autor der Studie

Tim Stuchtey, Christian Dörr, Enrico Frumento, Carlos Oliveira, Gianmarco Panza, Stefan Rausch, Johannes Rieckmann, Reda Yaich

Titel der Studie:

Versteckte Kosten nicht-vertrauenswürdiger Anbieter in 5G-Netzwerken

Herausgeber:

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Dr. Tim H. Stuchtey (V.i.S.d.P.)

ISSN: 2191-6756
BIGS Standpunkt Nr. 12, Dezember 2020

Titelbild: Sunshine Studio/Shutterstock.com

Copyright 2020 © Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH. Alle Rechte vorbehalten. Die Reproduktion, Speicherung oder Übertragung (online oder offline) des Inhalts der vorliegenden Publikation ist nur im Rahmen des privaten Gebrauchs gestattet. Kontaktieren Sie uns bitte, bevor Sie die Inhalte darüber hinaus verwenden.

Überarbeitung v3: Erstveröffentlichung 26.01.2021, überarbeitet 11.02.2021.

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Geschäftsführender Direktor:
Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telefon: +49-331-704406-0
Telefax: +49-331-704406-19

E-Mail: direktor@bigs-potsdam.org
www.bigs-potsdam.org

Versteckte Kosten nicht-vertrauenswürdiger Anbieter in 5G-Netzwerken

Tim Stuchtey, Christian Dörr, Enrico Frumento, Carlos Oliveira, Gianmarco Panza, Stefan Rausch, Johannes Rieckmann, Reda Yaich

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

VORWORT

In zahlreichen europäischen Ländern gibt es derzeit Diskussionen über die wirtschaftlichen Möglichkeiten im Zusammenhang mit dem neuen Mobilfunkstandard 5G. Dabei geht es um mögliche Produktivitätssprünge, aber auch die mit einer stärkeren Vernetzung verbundenen Sicherheitslücken und Abhängigkeiten, die sich ergeben würden, wenn diese neuen Mobilfunknetze mit chinesischer Technik gebaut würden. Bei einer anderen Gelegenheit nannten der Direktor des Hasso-Plattner-Instituts Christoph Meinel und ich Letzteres den „Huawei-Schock", in Anlehnung an den historischen Moment, als es den russischen Sputnik-Missionen gelang, den Westen zu erschüttern. Als Folge dieser Diskussionen haben einige Staaten chinesische Netzwerkausrüster vom Aufbau heimischer 5G-Netze ausgeschlossen oder die regulatorischen Hürden so hoch gesetzt, dass das Ergebnis einem Verbot gleichkommt.

Von den Netzausrüstern der 5G-Netze wird ein hohes Maß an Vertrauenswürdigkeit erwartet, um an dieser superkritischen Infrastruktur der Zukunft mitwirken zu können. Dazu gehören neben der technologischen Kompetenz auch ein unbeschadeter Ruf und die unbedingte Glaubwürdigkeit, sich den Gesetzen und Regeln des Landes zu unterwerfen, in dem sie die 5G-Netze aufbauen wollen. Für chinesische Anbieter ist es besonders schwierig diese Glaubwürdigkeit aufzubauen, weil sie ihren Hauptsitz in einem Land mit einer gelenkten Staatswirtschaft haben, das von Unternehmen bedingungslosen Gehorsam verlangt, das eine erschreckende Bilanz in Sachen Rechtsstaatlichkeit aufweist und das laut westlichen Geheimdiensten, Cybersecurity-Firmen und Medienberichten das Ursprungsland für zahlreiche Versuche von Wirtschaftsspionage ist.

Wenn Unternehmen mit einer solchen Herkunft dennoch am Aufbau von 5G-Netzen in Europa beteiligt werden, ist dies mit erheblichen Kosten verbunden. Nur ein Teil dieser Kosten fällt bei den Mobilfunknetzbetreibern an, die über ihre Netzanbieter entscheiden können. Ein Großteil der Kosten muss hingegen von anderen Teilen der Gesellschaft getragen werden, wie z.B. den Telekommunikationskunden oder den Steuerzahlern, die ohne weitere Regulierungen keinen Einfluss auf die Auswahl des Netzausrüsters haben. Außerdem fallen einige der Kosten erst lange nach dem Netzaufbau an und es besteht die Gefahr, dass diese bei der Investitionsentscheidung nicht hinreichend berücksichtigt werden.

In dieser Studie wollen wir die versteckten Kosten von nicht-vertrauenswürdigen Netzwerkanbietern aufzeigen und, soweit möglich, für vier europäische Länder (Deutschland, Frankreich, Italien, Portugal) berechnen. Für diese Aufgabe wurde ein hervorragendes, interdisziplinäres Projektteam zusammengestellt, das sich teilweise bereits aus anderen europäischen Forschungsprojekten kannte und schätzte. Seit dem Sommer arbeiten wir gemeinsam an diesem Thema - trotz der geografischen Trennung. Die ursprünglich geplanten Projekttreffen in Aveiro, Berlin, Mailand und Paris fielen leider der COVID-19-Pandemie zum Opfer. Gerade deshalb sind wir froh, dass unser Projekt nur durch zwei Geburten und nicht durch eine COVID-Erkrankung unterbrochen wurde.

Wir möchten uns bei den zahlreichen Experten, Kollegen und externen Mitarbeitern unserer Institutionen bedanken, die uns bei der Erstellung der Studie auf vielfältige Weise unterstützt haben. Unser ganz besonderer Dank gilt dem U.S. Department of State, das die Studie durch finanzielle Unterstützung ermöglicht hat. Für eventuelle Fehler in unserer Argumentation oder unseren Berechnungen sind ausschließlich die Autoren verantwortlich. Wir hoffen, mit dieser Studie einen konstruktiven Beitrag zur Entscheidungsfindung in unseren jeweiligen Heimatländern leisten zu können.

Dr. Tim H. Stuchtey

Dezember 2020

ZUSAMMENFASSUNG

In einigen europäischen Ballungsräumen kann man bereits ein 5G-Symbol auf dem Handydisplay erkennen. Dennoch befinden sich die meisten Netze noch in der Planungsphase und die Mobilfunknetzbetreiber haben noch nicht final entschieden, von welchem Anbieter sie die Netztechnik beziehen werden. Oft scheint es aber so, dass sie die Netze zumindest teilweise mit der Technik chinesischer Hersteller bauen wollen, es sei denn, staatliche Regulierungen oder ihr Kundenstamm verlangen etwas Anderes.

In diesem Beitrag beschreiben wir, warum die Sicherheit von 5G-Netzen für die Wirtschaft von größerer Bedeutung ist, als es bei 4G der Fall war. Wir definieren die Kosten, die durch den Aufbau der Netze mit nicht-vertrauenswürdiger Technologie entstehen können, und versuchen diese so gut wie möglich zu messen. Am Ende der Studie fassen wir Länderstudien für unsere Heimatländer Deutschland, Frankreich, Italien und Portugal in der Anlage zusammen.

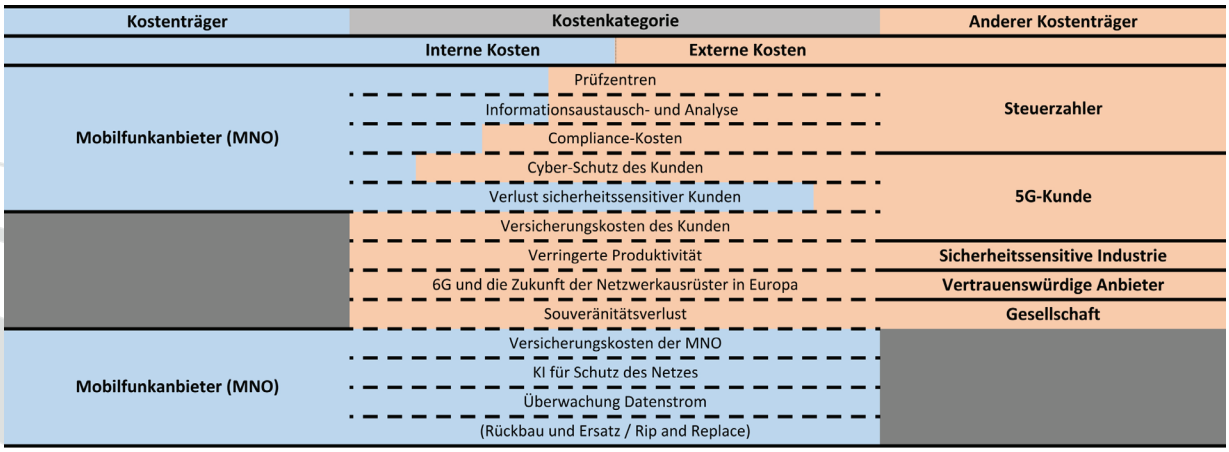
Chinesische Anbieter gelten vielfach als vertrauensunwürdig, weil sie aus einem Land ohne hinreichende Rechtsstaatlichkeit operieren, das strenge staatliche Kontrolle über ihr Geschäftsgebaren und Management ausübt. Das mangelnde Vertrauen in diese potenziellen Anbieter von 5G-Netztechnologie muss mit mehr Überwachung über das Netz bzw. die Daten, die durch dieses laufen, kompensiert werden. Aufgrund der wiederkehrenden Aktualisierung der 5G-Netzwerke werden diese Kontrollkosten während des gesamten Lebenszyklus des Netzwerks anfallen.

Bei der Entscheidung von welchen Anbietern 5G-Netztechnologie beschafft wird, berücksichtigen Mobilfunknetzbetreiber nicht alle Kosten. Das kann daran liegen, dass es sich um versteckte Kosten handelt, die später anfallen (**Lebenszykluskosten**) oder weil sie von anderen als den Mobilfunknetzbetreibern getragen werden (**externe Kosten**).

Einige der identifizierten Kosten werden auch dann anfallen, wenn 5G-Netzwerke nur mit vertrauenswürdiger Technologie aufgebaut werden. Diese Kosten werden jedoch geringer sein, da ein vertrauenswürdiger Anbieter ein kooperierender Partner bei der Absicherung des Netzwerks vor äußeren Einflüssen ist.

Die in der Studie definierten verborgenen Kosten können den Lebenszykluskosten und den externen Kosten zugewiesen werden, wie in der folgenden Tabelle dargestellt. Einige der Kosten sind sowohl externe als auch Lebenszykluskosten. Die externen Kosten, die von anderen Stakeholdern als den Mobilfunknetzbetreibern getragen werden, sind ebenfalls in der folgenden Tabelle 1 aufgeführt.

Tabelle 1: Art der versteckten Kostenkategorien - externe und Lebenszykluskosten.



Alle diese Kosten - mit Ausnahme der Versicherungskosten der Kunden, des Produktivitätsverlusts, 6G und der Zukunft der Netzwerkausrüster in Europa, und des Souveränitätsverlusts - , sind gleichzeitig **Lebenszykluskosten**, was bedeutet, dass sie nach dem Aufbau der 5G-Netze anfallen werden, oder **externe Kosten**, was bedeutet, dass die Kosten von jemand anderem als dem MNO getragen werden. Diese beiden Merkmale bilden die Nebelwand, hinter der **versteckte Kosten** nur schwer zu erkennen sind.

Quelle: eigenes Diagramm.

Wenn nicht-vertrauenswürdige Anbieter Teil eines 5G-Netzwerks sind, müssen zusätzliche Anstrengungen unternommen werden, um die bereitgestellten Software-Updates zu testen und zu überprüfen. Jedes Problem mit dem Netzwerk, das durch die Netzwerktechnologie verursacht wird, sollte mit anderen Mobilfunknetzbetreibern, staatlichen Stellen, die für Netzwerk- und Cybersicherheit zuständig sind, und mitunter auch den Kunden ausgetauscht werden. Neue Informationsaustausch- und Analysezentren (sog. ISACs) sollten im Inland und auf EU-Ebene eingerichtet werden. Es müssen zusätzliche Sensoren in das Netzwerk eingebaut werden, um den Netzwerkverkehr zu überwachen und unbeabsichtigte Datenflüsse an Dritte zu erkennen. Neue KI-Tools müssen entwickelt und in das Netzwerkmanagement als Frühwarnsystem für verdeckte Datenexfiltration integriert werden. Regierungen, Mobilfunknetzbetreiber und ihre Kunden werden Ressourcen für die Formulierung, Beeinflussung und Durchsetzung von Regulierungsrichtlinien und deren Einhaltung aufwenden müssen, um das fehlende Vertrauen in das Netz zu kompensieren. Zur Deckung von Schäden, die durch Cyberangriffe mit Hilfe von 5G-Netzen entstehen, müssen die Mobilfunknetzbetreiber und ihre Kunden (mehr) Geld für Cyberversicherungen ausgeben, um die finanziellen Folgen zu bewältigen. Kunden, die besonders auf den Schutz ihrer Daten bedacht sind (oder sein müssen), werden auf die Nutzung von Netzen mit vertrauensunwürdigen Anbietern verzichten und ihr Geschäft woanders hin verlagern. Wenn der Ruf eines nicht-vertrauenswürdigen Anbieters beschädigt wird, weil zusätzliche Beweise dafür vorliegen, dass er mit staatlich geförderten Cyberkriminellen zusammenarbeitet, muss die nicht-vertrauenswürdige Technologie schnell ersetzt werden, mit allen damit verbundenen Kosten (Rip-and-Replace), einschließlich eventueller vorübergehender Netzwerkabschaltungen.

Wenn das 5G-Netz vertrauensunwürdige Technologie enthält, fällt zudem ein größerer Teil der Last zum Schutz der Daten oder Maschinen, die über das Netz gesteuert werden, auf den 5G-Kunden. Dieser muss mehr Ressourcen für klassische Cybersicherheitswerkzeuge aufwenden oder auf die Nutzung des Netzwerks verzichten und kann somit potenzielle Produktivitätsgewinne nicht realisieren. Europäische Anbieter werden es schwer haben, mit Unternehmen zu konkurrieren, die im 5G-Geschäft keinen Gewinn erwirtschaften müssen. Selbst wenn sie im 5G-Geschäft bleiben, werden ihnen die Ressourcen für Forschung und Entwicklung fehlen, insbesondere wenn es um die Entwicklung der nächsten Generation von Mobilfunknetzen für das Jahr 2030 geht, wenn der Westen vollständig von chinesischer Netzwerktechnologie abhängig sein könnte. Regierungen, deren Wirtschaft vom Funktionieren nicht-vertrauenswürdiger Netzwerke abhängt, werden sich zweimal überlegen, ob und wann sie China in internationalen Konflikten herausfordern. Der politische Handlungsspielraum wird dadurch eingeschränkt.

Um die externen Kosten und den notwendigen zusätzlichen Schutz zu internalisieren, ist eine Regulierung notwendig, die entweder nicht-vertrauenswürdige Anbieter vom Aufbau von 5G-Netzen ausschließt oder von Mobilfunknetzbetreibern verlangt, in den notwendigen zusätzlichen Schutz zu investieren, wenn sie nicht-vertrauenswürdige Technologie verwenden. Auch wenn wir nicht herausfinden konnten, ob und um wieviel nicht-vertrauenswürdige Anbieter ihre Technologie in den vier von uns analysierten Ländern tatsächlich billiger anbieten als ihre vertrauenswürdigen Konkurrenten, werden die Kosten, die mit dem zusätzlich erforderlichen Schutz verbunden sind, höchstwahrscheinlich jeden Kostenvorteil, den die nicht-vertrauenswürdigen Anbieter haben, überwiegen.

INHALTSVERZEICHNIS

VORWORT 4

ZUSAMMENFASSUNG 5

1 EINLEITUNG 9

2 WARUM IST 5G SO WICHTIG? 11

2.1 Neue Anwendungsmöglichkeiten 12

2.2 5G Systemanforderungen 14

2.3 5G-Infrastruktur und ihre Komponenten 16

3 DIE BEDEUTUNG VON VERTRAUEN BEI 5G 17

4 DIE ROLLE DER SICHERHEIT BEI 5G 19

4.1 Technische Infrastruktur und das zukünftige Ausmaß der Abhängigkeit von 5G 20

4.2 Sicherheit und die Wahl des 5G-Netzwerkausrüsters 22

5 DIE OFFENSICHTLICHEN KOSTEN VON BÖSWILLIGEN NETZWERKAUSRÜSTERN IN 5G-NETZEN 24

6 DIE VERSTECKTEN KOSTEN VON NICHT-VERTRAUENSWÜRDIGEN NETZWERKAUSRÜSTERN IN 5G-NETZEN 26

6.1 Der ökonomische Charakter von Sicherheit 26

6.2 Prävention und Kontrolle 28

6.2.1 Technologie 28

6.2.2 Cyberbedrohungsanalyse 30

6.2.3 Prüfzentrum für 5G-Netzwerke und Anwendungen mit nicht-vertrauenswürdiger Technologie 31

6.2.4 Künstliche Intelligenz in 5G-Netzen 33

6.2.5 Regulierungskosten 36

6.2.6 Versicherung gegen Cyberrisiken 38

6.3 Verschiebung der Nachfrage 40

6.4 Veränderung der Angebotsseite 44

6.4.1 OpenRan und die Auswirkungen auf das Angebot 45

6.4.2 Marktstrukturen 46

6.5 Produktivitätskosten 47

7 KOSTEN FÜR DIE REAKTION NACH EINEM STÖRFALL 49

7.1 Untersuchung und Zuordnung 50

7.2 Schadensbewertung 50

7.3 Rip-and-Replace 53

8 FAZIT UND SZENARIEN 55
8.1 Optimistisches Szenario 56
8.2 Pessimistisches Szenario 56
8.3 Realistisches Szenario 58
9 ANHANG:
SYNTHESE DER LÄNDERSTUDIEN FÜR FRANKREICH, DEUTSCHLAND, ITALIEN UND PORTUGAL 60
9.1 Einleitung 60
9.2 Die 5G-Landschaft in Deutschland, Frankreich, Italien und Portugal 61
9.2.1 Deutschland 61
9.2.2 Frankreich 61
9.2.3 Italien 62
9.2.4 Portugal 63
9.2.5 Zusammenfassung 63
9.3 Veränderung der Angebotsseite: die Kosten für das Verbot von nicht-vertrauenswürdigen Anbietern 64
9.4 Offensichtliche Kosten von nicht-vertrauenswürdigen Anbietern nach Land 66
9.5 Die versteckten Kosten von nicht-vertrauenswürdigen 5G-Anbietern 68
9.5.1 Prüfzentren 68
9.5.2 Kosten von Datenschutzverletzungen 69
9.5.3 Verlust von sicherheitssensiblen Kunden - Verschiebung der kommerziellen Nachfrage 70
9.5.4 Verlust von sicherheitssensiblen Kunden - Verlagerung der Nachfrage der Regierung & redundante Infrastruktur 71
9.5.5 Kosten von Rip-and-Replace 72
TABELLEN- UND ABBILDUNGSVERZEICHNIS 73
QUELLENVERZEICHNIS 74
AUTOREN 79

1 EINLEITUNG

5G gilt als transformative Technologie, die schon bald die Basis für eine hohe Produktivitätssteigerung sein wird. In mehreren Ländern sind 5G-Netze bereits verfügbar und bieten zunächst wesentlich höhere Downloadraten als 4G/LTE. In Zukunft werden jedoch aufgrund der erhöhten Kapazität, der hohen Geschwindigkeit und der geringen Latenz neue Dienste aus dieser Generation von Mobilfunksystemen hervorgehen. Viele bestehende Industrien werden einen zunehmenden Teil ihrer Wertschöpfungskette digitalisieren und Produktion und Dienstleistungen über Mobilfunknetze laufen lassen, wodurch die 5G-Netze zu einer quasi überkritischen Infrastruktur werden.

Es gibt ein Sprichwort unter Sicherheitsforschern, das besagt: Wenn eine innovative Technologie nicht zuerst von Kriminellen missbraucht wird, ist sie wahrscheinlich nicht so innovativ. Die Verbindung von immer mehr Aspekten unseres Lebens und unserer Wirtschaft mit dem Internet bedeutet, dass unzählige neuer Angriffsvektoren für böswillige Akteure eröffnet werden. Gleichzeitig wird unsere Gesellschaft immer abhängiger von der Integrität und Verfügbarkeit, aber auch von der Vertrauenswürdigkeit, dieser neuen Netzwerke.

Die für den Aufbau dieser Netzwerke notwendige Ausrüstung stammt von einer Handvoll von Unternehmen. Nach einer intensiven Phase der Konsolidierung in der Netzwerkindustrie gibt es derzeit fünf relevante Anbieter auf dem Markt: Huawei, Ericsson, Nokia, ZTE und (als Neuling) Samsung. Diese Unternehmen liefern die Technik für Mobilfunknetze, die national von noch weniger primären Mobilfunknetzbetreibern betrieben werden. Diese Mobilfunkbetreiber bekommen von ihren Regierungen die entsprechenden Frequenzen für ihren Betrieb zugewiesen. In den meisten Ländern wurden die Frequenzen vom Staat in Bündeln versteigert und von den Telekommunikationsbetreibern gekauft, die dann die Netztechnik beschaffen, um sie nutzbar zu machen.

Wenn alle fünf Anbieter von Mobilfunknetzen die gleichen Funktionalitäten und Dienste anbieten, sollte der Preis für die Netzwerkausrüstung bei sonst gleichen Bedingungen, von Anbieter zu Anbieter gleich sein, so die grundlegende Wirtschaftstheorie. In der Realität scheinen chinesische Anbieter ihr Produkt aber zu einem deutlich niedrigeren Preis anzubieten als ihre westlichen Konkurrenten. In einigen Fällen ist der Preis so niedrig, dass er vermutlich nicht einmal die Produktionskosten deckt. Was ist der Grund für solche Angebote, und warum verhalten sich diese Unternehmen nicht so, wie es private, gewinnmaximierende Firmen normalerweise tun?

Für den Netzbetreiber sind die anfänglichen Kosten für den Aufbau des Netzes nur eine von vielen Ausgaben. Da während der Lebensdauer eines 5G-Netzes häufige Upgrades und Erneuerungen der Hard- und Software des Netzes notwendig sind, sind die Lebenszykluskosten tatsächlich relevanter als die anfänglichen Anschaffungskosten. Es ist auch wichtig herauszufinden, ob alle Kosten, die mit dem Aufbau, der Wartung und dem Betrieb eines Mobilfunknetzes verbunden sind, vom Betreiber getragen werden und somit bei der Entscheidung berücksichtigt werden. Einige der Kosten könnten externe Kosten sein, die entstehen, wenn die Produktion oder der Konsum eines Gutes oder einer Dienstleistung einem Dritten Kosten auferlegt. Wenn mit der Bereitstellung eines 5G-Netzes negative externe Effekte verbunden sind, werden die gesellschaftlichen Kosten größer sein als die privaten Kosten des Netzbetreibers. Die folgende ökonomische Analyse wird hoffentlich einen Beitrag zu dieser Debatte leisten.

Aufgrund des superkritischen Charakters der 5G-Netzwerke für unsere Wirtschaft und Gesellschaft in den nächsten Jahren sind Funktionalitäten und Servicepreise nicht die einzigen Aspekte, die bei der Auswahl eines Netzwerkanbieters zu berücksichtigen sind. Um die Vertraulichkeit und Integrität des Netzwerks und der darin enthaltenen Daten zu gewährleisten, ist es von entscheidender Bedeutung, dass der Mobilfunknetzbetreiber versteht, was das Netzwerk tut, und die volle Kontrolle über den Netzwerkverkehr hat. Falls er diese Kontrolle nicht hat, wird er für den Schaden, der durch sein Netzwerk ermöglicht wird, finanziell oder zumindest politisch haftbar.

Bei 5G-Netzen werden viele der Funktionalitäten, die in früheren Netzgenerationen auf Ad-hoc-Hardware implementiert wurden, nun durch Software realisiert, die auf Allzweck-Hardware läuft. In naher Zukunft werden diese auch auf offenen Plattformen realisiert. Die Software muss ständig aktualisiert werden, da sie im Laufe der Zeit immer mehr Funktionalitäten bieten wird.

Die Milliarden Zeilen von Code, die ein Netzwerk bilden, können von den Netzwerkbetreibern nicht vollständig verstanden und kontrolliert werden. Selbst Regierungsstellen und große Forschungsinstitute können dies nur für Teile des Netzwerks nachbilden. Folglich müssen Netzwerkbetreiber und Kunden den Netzwerkanbietern vertrauen können, dass ihre Geräte nur das leisten, was sie sollen, und nichts darüber hinaus. Sie müssen auch darauf vertrauen, dass niemand anderes als der Netzbetreiber das Netz kontrolliert. Wenn das Vertrauen in den Anbieter nicht ausreicht, wirkt das Vertrauen in das Rechtssystem und in die finanzielle Haftung des Anbieters als Sicherheitsnetz.

Vertrauen ist schwer zu messen, aber die Rechtsstaatlichkeit in einem Land ist ein gutes Maß für das ordnungsgemäße Funktionieren des Rechtssystems und die Möglichkeit, finanzielle Ansprüche durchzusetzen. Von den fünf Unternehmen, die 5G-Netze anbieten, haben drei ihren Sitz in Ländern, in denen die Rechtsstaatlichkeit laut dem Rechtsstaatlichkeitsindex 2020[1] des World Justice Program zu den höchsten Werten zählt: Finnland (Platz 3), Schweden (Platz 4) und die Republik Korea (Platz 17). Zwei Anbieter kommen aus China, das auf Platz 88 der 128 gerankten Länder liegt. China schneidet in diesem Ranking besonders schlecht ab, wenn es um unzulässige staatliche Einflussnahme auf das zivile Rechtssystem (Platz 122), Einschränkungen der staatlichen Befugnisse (Platz 123) und Grundrechte (Platz 126) geht.

Klas Friberg, der Leiter des schwedischen Geheimdienstes, sagt deswegen: *"The Chinese state carries out cyber espionage in order to promote its own economic development and to develop its military capability. It does so through comprehensive intelligence collection and theft of technology, research and development. This is something we have to take into account as the 5G network is being built. We cannot make compromises when it comes to Sweden's national security."*[2]

Ähnliche Kommentare können von anderen europäischen Geheimdienstmitarbeitern zitiert werden. Darüber hinaus identifizierte CrowdStrike, ein US-amerikanisches Unternehmen für Cybersicherheitstechnologie, China als *„the most prolific nation-state threat actor during the first half of 2018"*[3]. Der stellvertretende US-Justizminister John C. Demers erklärte bei einer Anhörung im Senat, dass China von 2011 bis 2018 mit mehr als 90 % der Fälle des US-Justizministeriums im Zusammenhang mit Wirtschaftsspionage und zwei Dritteln der Fälle von Geschäftsgeheimnissen in Verbindung gebracht wird.[4]

Es wäre daher naiv zu glauben, dass die Implementierung einer Technologie mit so vielen Möglichkeiten zur Untergrabung der Integrität und Vertraulichkeit von Daten sowie der Möglichkeit zur Sabotage durch nicht-vertrauenswürdige Anbieter nicht mit versteckten Kosten verbunden sei. In dieser Studie werden wir versuchen, diese Kosten zu benennen, zu definieren und zu messen - oder besser gesagt zu schätzen - für Deutschland, Frankreich, Italien und Portugal. Auf diese Weise hoffen wir, denjenigen, die für die Beschaffung von 5G-Technologie verantwortlich sind, und denjenigen, die den Markt regulieren, zusätzliche Informationen für ihre Entscheidungsfindung zu geben. Diese Informationen sollen auch dazu beitragen, dass sie dem Rat des chinesischen Präsidenten Xi folgen, der bei einer Internetkonferenz sagte: *"we should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing."*[5]

Eilige Leser, die bereits mit 5G und den Auswirkungen auf die Wirtschaft vertraut sind und ein Grundverständnis haben, wie 5G technisch funktioniert, können Kapitel 2 überspringen. Wenn man die Bedeutung des Vertrauens in die Technologie (Kap. 3) und die

1 World Justice Report (2020).
2 Säkerhetspolisen (2020).
3 Crowdstrike (2019).
4 Demer (2018).
5 Xi (2015).

Sicherheitsauswirkungen von 5G (Kap. 4) verstanden hat, kann man direkt zu den Kapiteln über die offensichtlichen (Kap. 5) und versteckten Kosten (Kap. 6) von 5G springen. In Kapitel 7 beschreiben wir die Kosten, die entstehen, wenn die Befürchtungen über nicht-vertrauenswürdige Anbieter bestätigt werden. Wir schließen mit drei Szenarien und deren wirtschaftlichen Folgen, bevor wir versuchen, dieses Konzept auf Deutschland, Frankreich, Italien und Portugal anzuwenden (Anhang Kapitel 9).

2 WARUM IST 5G SO WICHTIG?

Die erste Generation der drahtlosen zellularen Netzwerke[6] 1G, die 1979 in Japan eingeführt wurde, bot analoge Sprachdienste, während 2G, das 1991 eingeführt wurde, diese durch digitale Sprach- und SMS-Dienste ersetzte. 3G, eingeführt im Jahr 2001, bot ausreichende Datenraten für die ersten wirklich effektiven mobilen Internetdienste. Das 2009 eingeführte 4G wurde von Grund auf für schnelles mobiles Internet entwickelt und ermöglichte die Smartphone-Revolution und die App-Economy (siehe Tabelle 2 unten).

Mit dem Übergang zu großflächigen Implementierungen vom omni-vernetzten Internet der Dinge sind diese bestehenden Mobilfunknetze nicht mehr ausreichend. Prognosen gehen davon aus, dass die Zahl der weltweit vernetzten Geräte bis 2025 auf 55 Milliarden ansteigen wird.[7] Diese werden in den Bereichen Landwirtschaft, Fertigung, Gesundheit und Umweltsensorik zum Einsatz kommen, aber auch neue Dienste und Anwendungen im Verkehrswesen, wie selbstfahrende Autos, ermöglichen. Der drastische Anstieg der Geräte pro Quadratkilometer und das Aufkommen neuer Dienste mit unterschiedlichen Bandbreiten- und Latenzanforderungen sowie die Omnipräsenz der Maschine-zu-Maschine-Kommunikation sind mit der bestehenden 4G-Infrastruktur nicht mehr zu realisieren.

5G ist also nicht nur eine Entwicklung hin zu mehr Bandbreite, sondern ein Paradigmenwechsel in der Art und Weise, wie mobile Kommunikationsnetze aufgebaut sind. Die entscheidenden Innovationen von 5G finden nicht nur am Rand des Netzes statt, wo die Verbindung zwischen dem mobilen Endgerät und dem Mobilfunkmast hergestellt wird, sondern überwiegend im Kern und im Management des Telekommunikationsnetzes. In den folgenden Abschnitten werden wir kurz die neuen Wertversprechen, die daraus resultierenden Anforderungen und das High-Level-Design von 5G-Netzen diskutieren.

Tabelle 2: Entwicklung der Mobilfunknetze - Up- und Downloadgeschwindigkeiten

	1G	2G	3G	4G	5G
Approximate deployment date	1980s	1990s	2000s	2010s	2020s
Theoretical download speed	2kbit/s	384kbit/s	56Mbit/s	1Gbit/s	10Gbit/s
Latency	N/A	629 ms	212 ms	60-98 ms	< 1 ms

Source: ITU 2018, p. 6.

6 Zellulare Netzwerke bestehen aus vielen Sende- und Empfangsantennen, die jeweils eine Kommunikations-"Zelle" um sich herum bilden, mit der sich Telefone und Geräte verbinden können. Vielfach über eine Landschaft repliziert, bieten sie eine flächendeckende, nahtlose Abdeckung für die Verbindung von Geräten.

7 IDC (2020). https://www.idc.com/getdoc.jsp?containerId=prAP46737220#:~:text=IDC%20predicts%20that%20by%202025,from%2018.3%20ZB%20in%202019

2.1 Neue Anwendungsmöglichkeiten

Im Vergleich zu 4G ermöglicht 5G die 10 bis 100-fachen Datenübertragungsraten, nur ein Zehntel der Latenzzeit (die „Nachlaufzeit", die Geräte benötigen, um miteinander zu kommunizieren), eine weitaus größere Bandbreite und die 10-fache Anzahl an Geräten, die in einem bestimmten Gebiet vernetzt werden können (siehe Tabelle 3). Darüber hinaus ist die Technologie pro übertragenem Datenbit energieeffizienter.

Tabelle 3: Technische Merkmale und Vorteile von 5G im Vergleich zu 4G

	Latency	Peak data rates	Download speeds (Mbps)	Connections/ km2	Available spectrum	Illustrative antenna coverage (km)
4G	10ms	1Gb/s	1000	100k	3 GHz	50-150 (Mobile) 1-2 (Fixed wireless)
5G	<1ms	20Gb/s	10000	1m	30 GHz	50-80 (Mobile) 0.25-0.30 (Fixed Wireless)

Quelle: Kim (2019) und Singaligum (2019).

5G öffnet nicht nur die Tür zu besseren mobilen Kommunikationsdiensten für Einzelpersonen und Unternehmen, sondern auch für die Verbindung von Millionen, wenn nicht Milliarden von Maschinen - die Explosion des Internets der Dinge in verschiedenen Umgebungen (siehe Abbildung 1 unten). Die Internationale Fernmeldeunion (ITU) hat drei richtungsweisende, generische Anwendungsfälle identifiziert:

- **Erweitertes mobiles Breitband**. Als Weiterentwicklung der primären Nutzung von 4G, das durch die höheren Geschwindigkeiten ermöglicht wird, wird 5G "enhanced indoor and outdoor broadband, enterprise collaboration, and augmented and virtual reality" ermöglichen, typischerweise für Einzelpersonen.

- **Massive maschinenbasierte Kommunikation.** Ein neuer Anwendungsfall: Die hohe Bandbreite von 5G wird es Millionen von Sensoren und Maschinen ermöglichen, sich zu verbinden und Daten untereinander und mit der Organisation, zu der sie gehören, auszutauschen. Dies ermöglicht eine weitaus größere Effizienz und Effektivität von Dienstleistungen, Unternehmen und sogar „intelligenter" Infrastruktur. Zu den Anwendungen gehören eine deutlich effizientere und reaktionsschnellere Logistik, der Betrieb von Verkehrsknotenpunkten, die Steuerung des Verkehrsflusses und die Kontrolle des Stromnetzes.

- **Ultrazuverlässige und latenzarme Kommunikation.** Durch die sehr geringe Latenz, die 5G bietet, können Sensoren und Maschinen, die von Organisationen betrieben werden, die zeit- und sicherheitskritische Anwendungen bereitstellen müssen, verbunden werden und erstmals zusammenarbeiten. Zu den Anwendungen gehören autonomes Fahren, medizinische Fernoperationen und das Management kritischer nationaler Infrastrukturen.[8]

5G hat Vorteile für andere Technologie- und Innovationsbereiche, die derzeit entwickelt werden, und wird von diesen stark profitieren. Laut ITU ist 5G eine der fünf Säulen der digitalen Transformation, zusammen mit IoT, Alternate/Virtual Reality, Cloud-Diensten und Künstlicher Intelligenz (KI). Im Bereich der KI wird 5G beispielsweise die Anzahl der verfügbaren Sensoren deutlich erhöhen und riesige Datenmengen bereitstellen, die für das Training der maschinellen Lernalgorithmen, die das Herzstück der KI-gestützten Systeme bilden, entscheidend sind. Mit neuen Datenquellen entstehen auch neue KI-basierte Dienste und Geschäftsmodelle.[9]

Das bedeutet, dass wir wahrscheinlich beachtenswerte neue Bereiche des Nutzens und der Produktivitätssteigerung für Unternehmen und Gesellschaft rund um 5G entstehen sehen werden:

8 ITU (2018), S. 6.
9 Taulli (2020).

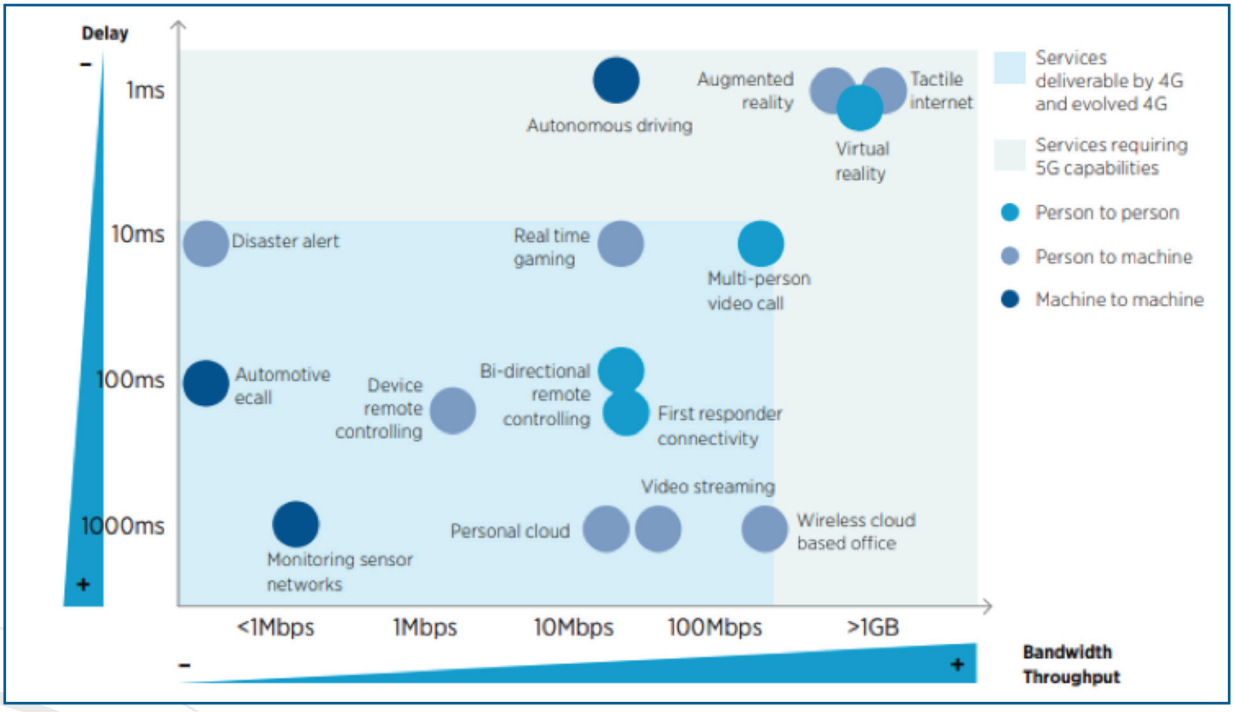
- Intelligenter Transport: Die 5G-Fahrzeugkonnektivität ermöglicht es Fahrzeugen, sich untereinander, mit der Infrastruktur, mit Netzdiensten und mit anderen Verkehrsteilnehmern zu verbinden. Dies kann zu einer effizienteren und sichereren Straßennutzung führen. 5G macht wirklich automatisierte Fahrzeuge möglich.[10]

- Intelligente Städte: Als Schlüsseltechnologie für das Internet der Dinge bei der Steuerung von städtischen Verkehrssystemen, Energienetzen und kommunalen Dienstleistungen ermöglicht 5G die Vision von „Smart Cities".[11]

- E-Health: Hochauflösende Videokonsultationen, Assistenzroboter für die Chirurgie und intelligente Wearables wie Gelenkimplantate könnten dazu beitragen, die Effizienz und Effektivität von Behandlungen zu erhöhen, die Orte, an denen Behandlungen möglich sind, zu verändern, sowie die Verlagerung des Gesundheitswesens hin zu mehr präventiven Eingriffen unterstützen.[12]

- Industrie 5.0: 5G wird den Übergang von Industrie 4.0 zu 5.0 vorantreiben. Eine Revolution, in deren Mittelpunkt die Zusammenarbeit zwischen Menschen und Maschinen steht, mit dem Ziel, der Produktion einen Mehrwert zu verleihen, indem personalisierte Produkte geschaffen werden, die die Anforderungen der Kunden erfüllen.

Abbildung 1: 5G wird niedrige Latenzzeiten und hohen Durchsatz bei allen Diensten unterstützen



Quelle: GSMA (2019), S.31.

10 Nokia (2020a).
11 Behesti (2019); Hui et al. (2020).
12 Nokia (2020b).

Allein in wirtschaftlicher Hinsicht werden die Vorteile sehr wahrscheinlich enorm sein. Einigen Schätzungen zufolge wird 5G bis zum Jahr 2035 12,3 Billionen US-Dollar an globaler Wirtschaftsleistung generieren. Es wird erwartet, dass Investitionen in die 5G-Wertschöpfungskette bis zu diesem Zeitpunkt weitere 3,5 Billionen US-Dollar an Wertschöpfung generieren und 22 Mio. Arbeitsplätze finanziert werden.[13]

5G wird voraussichtlich in Zukunft auch eine wichtige Rolle im Bereich Sicherheit und Verteidigung spielen. Analysen zu den Auswirkungen von 5G für Strafverfolgungsbehörden und Nachrichtendienste sind begrenzt, aber wir finden Beispiele dafür, dass die 5G-Infrastruktur von Strafverfolgungsbehörden genutzt werden kann, um Personen und Vermisste[14] zu lokalisieren, und dass 5G für Rettungsdienste von der Leitstelle bis zur Frontlinie nützlich wird.[15]

Für das Militär sind die Vorteile, die 5G verspricht, noch offensichtlicher. Laut NATO-Analysten sollte die Allianz 5G-Technologien für die Befehls- und Kontrollfunktionen, die Kommunikation und andere militärische Zwecke verwenden und sie weisen auch darauf hin, dass es ohne 5G schwierig sein wird, Big Data, künstliche Intelligenz und Cloud Computing im Konfliktfall vollständig zu nutzen.[16] Das US-Militär treibt die Entwicklung bereits voran. So wurde kürzlich eine Finanzierung von 600 Mio. Dollar für 5G-Entwicklungen an fünf verschiedenen Militäreinrichtungen angekündigt.[17]So stellt das US-Verteidigungsministerium zu 5G fest: *"Ubiquitous high-speed connectivity will … transform the way militaries operate … the deployment of 5G capabilities will offer a host of opportunities to both reform DoD enterprise services and to create powerful new military advantages."*[18]

Die Auswirkungen auf Sicherheit und Verteidigung werden komplexer durch die Verteilung von Strafverfolgungsbehörden, Nachrichtendiensten, Verteidigung und Anbieter kritischer Infrastrukturen auf private und öffentliche 5G-Netze, welche schwer zu prognostizieren ist. Die Schwachstellen und Dilemmata, die 5G schaffen kann, sind Gegenstand des nächsten Abschnitts.

2.2 5G Systemanforderungen

Die neuen Anwendungsszenarien für das Mobilfunknetz der fünften Generation schaffen eine Reihe von neuen technischen Anforderungen. Um diese zu erfüllen, sind 5G-Netze einerseits auf weiterentwickelte und aufgerüstete Technologiekomponenten, andererseits aber auch auf ein anderes Designparadigma angewiesen. Im folgenden Abschnitt wird kurz erörtert, welche technischen Anforderungen durch diese Anwendungsfälle aus Sicht des Systems und seines Managements entstehen und wie diese im 5G-Ökosystem realisiert werden.

1. Hohe Datenrate und geringe Latenz: Wie oben gezeigt, hat jede neue Generation von Mobilfunknetzen eine deutliche Steigerung der maximalen und anhaltenden Bandbreite für den Endnutzer ermöglicht. Während 4G-Netze Spitzen-Datenraten von 1 Gbit/s und eine anhaltende Erlebnis-Bandbreite von etwa 10 Mbit/s bieten können, werden neue Dienste wie autonomes Fahren oder virtuelle Realität das, was von aktuellen Netzen zuverlässig bereitgestellt werden kann, bei weitem übersteigen. Innerhalb von 5G wird erwartet, dass sich die erlebte Datenrate um das 100-fache erhöht und bis zu 1 Gbit/s erreicht. Häufig haben diese Anwendungen auch intensive Anforderungen an die Datenverzögerung, zum Beispiel beim autonomen Fahren. Wenn Daten über Geräte hinweg geteilt werden müssen, sind Latenzen von 1 ms ein Ziel, was ein Zehntel dessen ist, was von aktuellen Mobilfunknetzen bereitgestellt wird.

2. Massive Konnektivität: Jedem angeschlossenen Gerät wird ein Stück der für die Basisstation verfügbaren Konnektivität zur Verfügung gestellt, sowohl in Form eines kleinen Zeitfensters als auch eines Teils des Frequenzspektrums. Bisher wurde das Netz hauptsächlich von Handynutzern verwendet

13 ITU (2018), S.8.
14 Roke (2020).
15 TechUK (2019).
16 Gilli und Bechis (2020).
17 The Hill (2020).
18 Department of Defense (DoD) (2020).

und nur ein Teil des Netzes wurde für die Maschinenkommunikation genutzt. Frühere Generationen von Mobilfunknetzen waren für eine begrenzte Anzahl solcher Zeitfenster ausgelegt, die durch die neuen Anwendungsfälle und die Verbreitung des Internet der Dinge, das über Mobilfunknetze verbunden ist, weit überschritten wird. Das neue Design von 5G trägt diesen neuen Anwendungsfällen Rechnung, indem es die Anzahl der anschließbaren Endpunkte pro Quadratkilometer um mehr als den Faktor 100 erhöht.

3. Energieeffizienz: Während bei bisherigen mobilen Anwendungen, die von Mobiltelefonen oder mobilen Endpunkten wie Auto-Uplinks genutzt wurden, der Energieverbrauch eine untergeordnete Rolle spielte, wird sich dies ändern, wenn die Vernetzung des Internet der Dinge in den Fokus rückt. Hier werden Low-Cost-Geräte in weiten Bereichen eingesetzt, was bedeutet, dass diese Einheiten über längere Zeiträume mit Batteriestrom betrieben werden müssen, da die Wartung und der Austausch von Batterien im Feld weder wirtschaftlich noch ökologisch sinnvoll sind. 5G wird den Energieverbrauch für die mobile Einheit drastisch reduzieren und sensorische Anwendungen ermöglichen, die 10 Jahre oder länger mit einer Batterie auskommen.

4. Programmierbarkeit: Da die 5G-Netzinfrastruktur darauf abzielt, eine Vielzahl von Diensten mit unterschiedlichen Leistungsanforderungen zu unterstützen, basiert die Systemarchitektur auf flexiblen Bausteinen, die individuell programmiert werden können. Dies kann auf verschiedenen Ebenen erfolgen: Dienste werden aufgeteilt und können unterschiedliche Datenzuweisungen und Sicherheitsstufen erhalten. So kann zum Beispiel eine eHealth-Anwendung in einer völlig anderen Zone betrieben werden, die frei von Störungen durch die normale Handynutzung ist. Diese Isolierung verschiedener Anwendungsfälle ermöglicht es, dass Dienste mit strengen Qualitätsanforderungen bedient werden können.

Foto © AerialPerspective Works/iStockphoto

2.3 5G-Infrastruktur und ihre Komponenten

Um diese neuen Anwendungen zu ermöglichen und ihre Anforderungen zu realisieren, führt 5G eine Reihe von Innovationen im Funkzugangsnetz (Radio Access Network - RAN) und im Netzwerkkern ein. Im folgenden Abschnitt wird eine Auswahl dieser technologischen Fortschritte kurz erläutert:

- Das 5G **Funkzugangsnetz (RAN)**: Das RAN, ist der Teil des Mobilfunknetzes, der mit den mobilen Nutzern interagiert, wobei die mobilen Basisstationen den sichtbarsten Teil bilden. Um Anwendungsfälle mit hoher Bandbreite und massivem Einsatz zu ermöglichen, nutzen 5G-Netzwerke ein größeres Frequenzband und insbesondere höhere Frequenzen als aktuelle 3G/4G-Installationen, da hohe Datenraten bei höheren, sogenannten Millimeterwellenfrequenzen effizienter übertragen werden können. Die Netzwerkkapazität und -dichte wird durch den Einsatz von MIMO (Multiple Input, Multiple Output) weiter erhöht, was bedeutet, dass mehrere Antennen gleichzeitig zum Senden und Empfangen von Daten an ein einzelnes Mobilgerät verwendet werden. 5G setzt auf massive MIMO - es werden also viele verschiedene Antennen für verschiedene Nutzer verwendet - und Beamforming, um den Durchsatz auf der Funkschnittstelle zu erhöhen. Da das Funkspektrum – bzw. die Kommunikationsfrequenzen - eine begrenzte und teure Ressource ist, erhöht 5G die Anzahl der Nutzer und Geräte, die unterstützt werden, indem es die Dichte der Zellen erhöht. Da jede Zelle von Funkzugangsknoten mit geringer Leistung betrieben wird, kann der Netzbetreiber dieselben Frequenzen über ein größeres Gebiet verwenden, da die Sendeleistung und damit potenzielle Störungen reduziert werden. Eine geringere Sendeleistung führt auch zu Energieeinsparungen und einer besseren Akkulaufzeit.

  Neben diesen Verbesserungen, die in der Interaktion zwischen der Mobilfunkbasisstation und dem Gerät des Teilnehmers stattfinden, gibt es auch große Veränderungen bei der Funktionsweise der Hardware im Funkzugangsnetz. Statt dedizierter Hardware, die die gesamte Funktionalität kapselt, entkoppeln Innovationen wie cloudRAN den abgesetzten Funkkopf - vereinfacht gesagt, den Sender/Empfänger des Mobilfunkturms - von der Basiseinheit, die die Signalverarbeitung übernimmt. Beide sind durch Hochgeschwindigkeits-Glasfasernetze miteinander verbunden und bieten dem Mobilfunkanbieter die Möglichkeit, letztere innerhalb einer Cloud-Computing-Umgebung zu betreiben. Das bedeutet, dass die Netze bei steigendem Bedarf leichter skaliert werden können und nicht mehr auf spezielle Hardware angewiesen sind, wodurch sie kostengünstiger zu betreiben sind. Bei den sehr hohen Anforderungen an Bandbreite und Latenz der neuen 5G-Dienste können diese nur erfüllt werden, wenn die Dienste näher an den Mobilfunknutzer heranrücken. Dies wird als Edge- oder Fog-Computing bezeichnet und ist möglich, weil viele Dienste durch Virtualisierung auf der gleichen Systemhardware bereitgestellt werden können.

  Es wird zuweilen argumentiert, dass das Funkzugangsnetz ein relativ unbedeutender Teil eines 5G-Netzes ist und die Vertraulichkeit und Integrität von 5G-Diensten nicht beeinflusst. Aus technischer Sicht ist dies jedoch ein Irrtum. Die 5G-Basisstation (gNB) ist der Endpunkt für Verschlüsselung und Integritätsschutz. Daher ist die Benutzerebene potenziell (für jeden, der Zugang zur Basisstation hat) im Klartext zugänglich, wenn keine Ende-zu-Ende-Verschlüsselung verwendet wird.[19] In diesem Zusammenhang sind die technischen Aspekte der Sicherheit in Funkzugangsnetzen ebenso kritisch wie das Kernnetz in Bezug auf Integrität und Vertraulichkeit.

- Das 5G-**Kernnetz**: Da das Netzwerk mehrere Dienste mit unterschiedlichen Serviceanforderungen gleichzeitig bereitstellen muss, nutzt 5G programmierbare Netzwerke um die Koexistenz und Flexibilität zu gewährleisten. Software Defined Networking (SDN) ist eine etablierte Technik in Rechenzentrumsnetzen und wird im Kontext von 5G eingesetzt, um einen agilen Kern zu erstellen, der an neue Anforderungen und neu eingeführte Dienste angepasst werden kann. Dies ermöglicht es Netzbetreibern, zusätzliche Dienste mit minimalem Aufwand bereitzustellen. Eine ähnliche Softwareisierung bietet die Netzwerkfunktionsvir-

19 Vgl. Ericsson (2020a).

tualisierung (NFV), bei der die Netzwerkfunktionalität nicht mehr mittels spezieller, dedizierter und damit teurer Hardware bereitgestellt wird, sondern durch Software auf Commodity-Servern, die eine einfachere Skalierung bei wechselnder Nachfrage sowie die Implementierung neuer Funktionen in schnelleren Bereitstellungszyklen und zu stark reduzierten Kosten ermöglichen.

5G nutzt diese Technologien, um Network Slicing zu realisieren. Dabei wird dieselbe physische Hardware in mehrere logische Kompartimente aufgeteilt, die jeweils unterschiedlichen Endnutzern (z. B. autonomes Fahren, eHealth, persönliche Mobiltelefone) mit unterschiedlichen Leistungs- und Sicherheitsanforderungen gewidmet sind. Dies garantiert eine vollständige störungsfreie Trennung verschiedener Anwendungen und Anwendungsfälle auf derselben Hardware, was Kosten spart und es den Netzwerken ermöglicht, viel einfacher als bisher mobile virtuelle Netzwerkbetreiber zu schaffen.

Um das volle Potenzial von 5G zu nutzen, sind sowohl ein aufgerüstetes Funkzugangsnetz, als auch ein aufgerüstetes Kernnetz erforderlich. Derzeit gibt es weltweit fast kein Mobilfunknetz, das „vollständig" 5G ist, d. h. in dem alle erforderlichen Komponenten sowohl im Kern als auch im Funkzugangsnetz eingesetzt werden. Die meisten Netze haben damit begonnen, ein verbessertes Funkzugangsnetz zu implementieren, in dem Massive MIMO oder kleinere Zellen bereits eine verbesserte Nutzerbandbreite im Vergleich zur 4G-LTE-Technologie bieten können, aber noch nicht die verschiedenen Anwendungsszenarien ermöglichen, die in einem „All-5G"-Netz möglich sind (siehe Tabelle 4).

Tabelle 4: Systemanforderungen aus Anwendungsfällen und technischer Realisierung in 5G

Systemanforderungen	Technische Realisierung in 5G
Hohe Datenrate, geringe Latenzzeit	Massive MIMO, Smaller Cells Edge Computing
Massive Konnektivität	Massive MIMO, Smaller Cells
Energieeffizienz	CloudRAN, Smaller Cells
Programmierbarkeit	CloudRAN, SDN, NFV, Network Slicing

Quelle: eigenes Diagramm.

3 DIE BEDEUTUNG VON VERTRAUEN BEI 5G

Sowohl in der Gesellschaft als auch in der Wirtschaft stellt Vertrauen ein grundlegendes Konzept für Menschen dar, ohne welches sie weder handeln noch interagieren können. Deshalb hat Abraham Maslow Vertrauen auf die zweite Ebene seiner Hierarchie der menschlichen Bedürfnisse gestellt, gleich nach dem physischen Bedarf für das menschliche Überleben. In der IT-/Cyberbranche hört man oft den Slogan: ***security builds trust and trust builds business.*** Doch wie können Telekommunikationsanbieter davon ausgehen, dass sie noch erfolgreich Geschäfte machen können, wenn das Vertrauen in ihr Netzwerk fehlt?

Vertrauen ist schwer zu definieren und zu quantifizieren, noch schwieriger als Sicherheit. Wirtschaftlich gesehen bedeutet Vertrauen eine Reduzierung der Transaktionskosten. Aufgrund von Vertrauen lassen wir in unserer Wachsamkeit nach und geben weniger für Kontrolle und Schutz aus. Gambetta definierte Vertrauen als *„a particular level of subjective probability with which a party A expects that another party B performs a given action, both before it can monitor such action and independently of its ability to monitor it."*[20]

In wenigen Jahren werden die Netzwerke der 5. Generation das Rückgrat unserer Gesellschaften und Volkswirtschaften bilden und Milliarden von Objekten und Systemen miteinander verbinden, darunter auch solche, die in kritischen Sektoren wie Energie, Transport, Gesundheitswesen, Banken und Industrie eingesetzt werden. Wenn ein Netzwerk, das einen so großen Einfluss auf unsere Gesellschaft und Wirtschaft hat, von Unternehmen aufgebaut und (teilweise) gewartet wird, die aus einem Umfeld mit schwacher Rechtsstaatlichkeit kommen, in dem grundlegende demokratische Prinzipien offen verletzt und geistige Eigentumsrechte missachtet werden, ist es schwer, Vertrauen aufzubauen. *„Trust but verify"* ist nicht nur ein Sprichwort, daher muss fehlendes Vertrauen mit verstärkten Anstrengungen für Schutz und Kontrolle kompensiert werden.

Vertrauenskonzepte, wie sie jetzt verstanden werden, reichen nicht aus, um komplexe 5G-Infrastrukturen zu verwalten. Das Vertrauen in 5G-Anbieter kann eine Vielzahl von Grundlagen haben. Man kann sich entscheiden, einem Anbieter aufgrund der Qualität seiner Produkte, aufgrund seines Rufs, oder aufgrund einer langjährigen Beziehung zu vertrauen. Auch die Möglichkeit, den Inhalt (Hardware und Software) der Geräte des Anbieters zu verifizieren, wird oft als Vertrauensgrundlage genutzt. Da es sich aber bei 5G-Netzen größtenteils um Software Defined Networks (SDN) handeln wird, die die Betriebs- und Wartungskosten für den Mobilfunknetzbetreiber senken und aufgrund von Software-Patching und -Updates unvergleichlich dynamischer sein werden als 4G-Netze, wird es auch immer schwieriger - wenn nicht gar unmöglich - werden, jede angepasste Softwareversion und -komponente auf kontinuierlicher Basis effektiv, effizient und rechtzeitig zu überprüfen. In einem wettbewerbs- und gewinnorientierten Umfeld wird die Überprüfung daher selektiv erfolgen müssen, während ein erheblicher Anteil der Softwareanpassungen aus Zeit-, Budget-, Personal- und anderen Ressourcengründen nicht kontrolliert werden kann.

In vielerlei Hinsicht lässt sich der Markt für 5G-Netzwerkhard- und -software als das beschreiben, was George Akerlof einen **Markt für Zitronen** nannte, d. h. ein Markt, in dem der Käufer nicht zwischen mehr oder weniger sicheren Netzwerkanbietern unterscheiden kann. Es besteht eine **Informationsasymmetrie** zwischen den beiden Seiten des Marktes.[21] Käufer wissen, wenn sie sich an einen Anbieter binden, nicht, ob sie einen Pfirsich (gute Qualität) oder eine Zitrone (niedrige Qualität) bekommen werden. Wenn Käufer einfach davon ausgehen, dass alle Anbieter das gleiche durchschnittliche Niveau an Netzwerksicherheit bieten (jedem Anbieter vertrauen), wird das Ergebnis sein, dass sich die Nachfrage zu dem Anbieter mit dem niedrigsten Preis und der geringeren Sicherheitsqualität verlagert. Letztendlich werden die qualitativ hochwertigeren und sichereren Anbieter den Markt verlassen, was zu einer **negativen Selektion hin zu Netzwerken mit niedriger Sicherheit** führt, mit enormen Konsequenzen nicht nur für den 5G-Markt und seine Anwendungen, sondern auch für die nächste Generation von Mobilfunknetzen (6G).

Vertrauen ist auch auf dem Markt für 5G-Dienste, bei dem die Mobilfunknetzbetreiber die Anbieter sind und die Nachfrage von Unternehmen, Regierung und Bürgern kommt, ein wichtiger Faktor. Die Kunden werden sehr wenig bis gar kein Wissen über das Innenleben eines 5G-Netzes haben, und auch hier können wir von einer großen Informationsasymmetrie ausgehen. Die Kunden werden den Mobilfunknetzbetreibern vertrauen müssen und ihnen das **Wohlwollen** entgegenbringen, das diese sich mit vergangenen Leistungen verdient haben. Dieses Wohlwollen kann jedoch leicht verloren gehen, sollte der Verdacht aufkommen, dass die Technologie nicht vertrauenswürdig ist. Und während es für einen Betreiber kostspielig sein wird, das Vertrauen wiederzugewinnen, ist ein Wechsel des Netzbetreibers für Kunden vergleichsweise einfach.[22]

20 Gambetta (1988), S. 216.

21 Akerlof, George A. (1970).

22 Für eine ausführlichere Diskussion über die Rolle von Vertrauen in der Cybersicherheit vgl. Lysne (2018), S. 11 ff.
Olav Lysne, The Huawei and Snowden Questions, Simula SpringerBriefs on Computing, Vol 4, Springer 2018. https://www.springer.com/gp/book/9783319749495

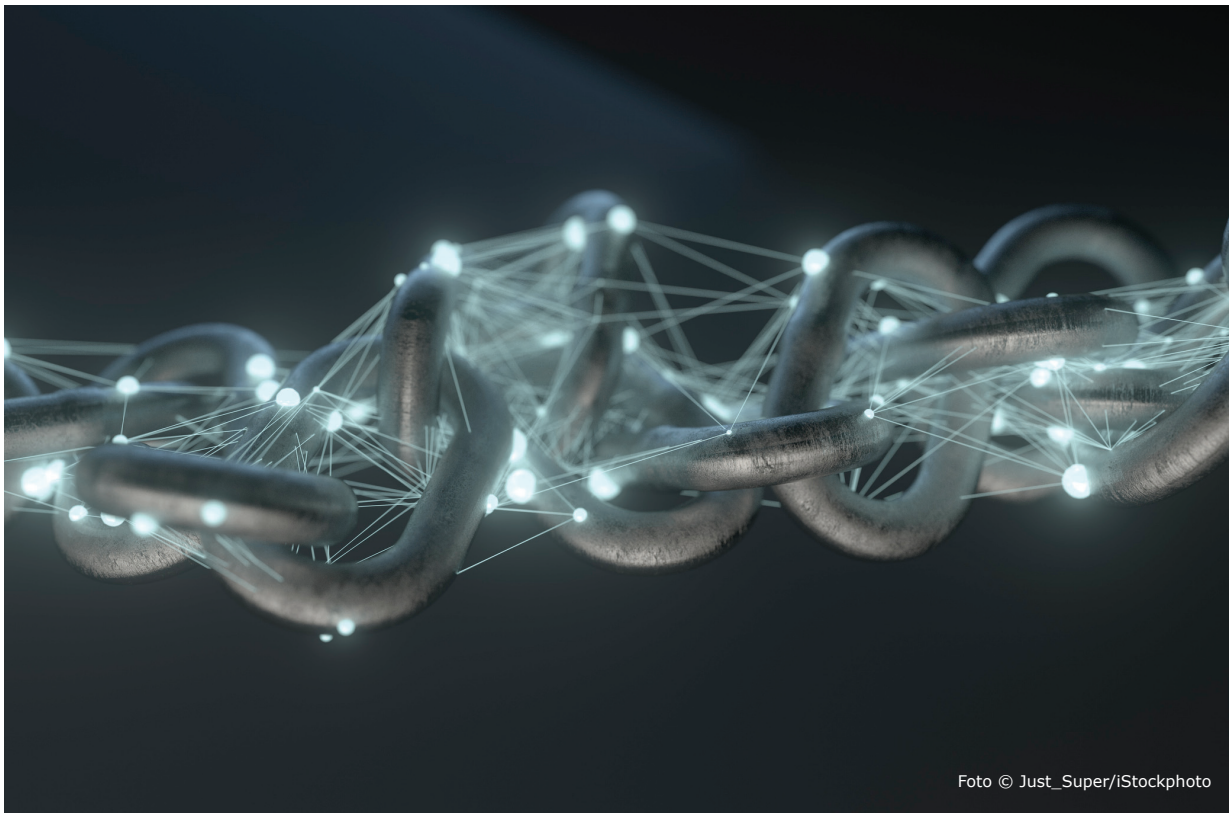


Foto © Just_Super/iStockphoto

4 DIE ROLLE DER SICHERHEIT BEI 5G

Keine Kommunikationstechnologie ist jemals vollständig sicher, und 5G bildet da keine Ausnahme: Es birgt erhebliche neue Schwachstellen und Herausforderungen.[23] Was 5G qualitativ von früheren Generationen der Telekommunikationstechnologien unterscheidet, ist, dass es zu einer neuen „superkritischen nationalen Infrastruktur" wird, von der wichtige Teile der Wirtschaft und der nationalen Infrastruktur (wie Wasserversorgung und Strom) abhängen werden.[24] Es ist auch ein Teil der Infrastruktur, über die in Zukunft die für die wirtschaftliche Gesundheit und die nationale Sicherheit wichtige Kommunikation stattfindet. Ein Cyberangriff auf Stromnetze wäre zum Beispiel verheerend.[25] Hacker üben bereits, wie sie ihr Handwerk an die Möglichkeiten von 5G anpassen können.[26] Es ist daher äußerst wichtig, dass Staaten die Sicherheitsaspekte berücksichtigen, bevor sie wichtige Entscheidungen zu 5G treffen.

Informationssicherheit besteht aus drei Elementen, die manchmal auch als **CIA-Dreiklang** bezeichnet werden: Vertraulichkeit, Integrität und Verfügbarkeit. Der Schwerpunkt der Schutzmechanismen in der klassischen Büro-IT und in der industriellen Forschung und Entwicklung lag früher auf dem Schutz der Vertraulichkeit. Doch mit dem Aufkommen von Industrie 4.0 und dem Internet der Dinge, befeuert durch die immer schnellere Vernetzung und Automatisierung von Produktionsanlagen, die durch die 5G-Infrastruktur ermöglicht wird, wird die Bedeutung der anderen beiden Elemente, Integrität und Verfügbarkeit, immer deutlicher.

23 Für einen Überblick über die 5G-Sicherheitsrisiken vgl. z. B. 5G PPP Security WG.
24 Cave (2020).
25 Lloyds (2015).
26 Wheeler (2019).

Unter **Vertraulichkeit** versteht man eine Beschränkung des Zugriffs und Einschränkung von Informationen. Vertraulichkeit wird im Rahmen von Industriespionage oder aus anderen Gründen für Abhörmaßnahmen gebrochen. Sie ist häufig von der Verletzung des geistigen Eigentums (intellectual property - IP) oder der Privatsphäre betroffen. Neben Wettbewerbsnachteilen, die für die Inhaber von geistigem Eigentum entstehen, stellen sich auch Haftungsfragen. Ist der Mobilfunknetzbetreiber für Diebstahl von geistigem Eigentum und Datenschutzverletzungen haftbar oder zumindest politisch verantwortlich zu machen? Mit dem steigenden Wert von Daten/Informationen in einer digitalen Wirtschaft steigt auch der Wert der Vertraulichkeit. Wenn die Eigentumsrechte an den Informationen nicht gewährleistet werden können, bedeutet dies, dass der Zugang zu diesen Daten nicht vollständig kontrolliert wird. Vertraulichkeit ist auch im Bereich der nationalen Sicherheit von großer Bedeutung. Der Austausch von Informationen zwischen Verbündeten ist gefährdet, wenn mindestens eine Regierung unsichere Kommunikationstechnologie benutzt.

Fragen der **Integrität** beziehen sich auf das Risiko der Manipulation von Inhalten. Eine böswillige Veränderung von Daten korrumpiert Datensätze und kann beispielsweise die Produktqualität in der Industrie 4.0-Fertigung sabotieren, zu Fehlern bei Geschäftsentscheidungen führen, die Lagerhaltung und Wartung stören und so weiter. Wenn 5G-gesteuerte Fabriken es einem Angreifer ermöglichen, die Integrität der Produktion zu kompromittieren, wird ein solches Werkzeug einen Wettbewerber viel mehr kosten als eine Störung der Produktion durch physische Gewalt. Oder aus der Sicht des Verteidigers: Es ist gut zu wissen, dass die Maschinen laufen, aber es ist noch wichtiger zu wissen, dass sie das produzieren, was sie produzieren sollen.[27]

Verfügbarkeit im Zusammenhang mit einem Mobilfunknetz bedeutet zunächst einmal, dass das Netz in Betrieb ist und funktioniert. Das Netz kann potentiell durch böswillige Parteien schrittweise eingeschränkt werden. Vorübergehende oder lokale bis regionale Verlangsamungen sind denkbar[28], und auch schwerwiegende Eingriffe bis hin zu kompletten Netzunterbrechungen (wie das Umlegen eines Kill Switches) sind im Falle eskalierender internationaler Konflikte nicht auszuschließen. Letzteres dürfte ein eher unwahrscheinliches Ereignis sein, da sie unweigerlich ein anschließendes Rip-and-Replace-Szenario auslösen würden. Ein Beispiel ist der massive Cyberangriff auf Estland 2007, vermutlich ausgeübt durch Russland. Seitdem hat die Abhängigkeit unserer Wirtschaft und Gesellschaft von digitalen Netzen nochmal dramatisch zugenommen

4.1 Technische Infrastruktur und das zukünftige Ausmaß der Abhängigkeit von 5G

Wie eingangs kurz erläutert, sind die Gründe für Risiken für die Sicherheit von 5G vielfältig und umfassen die technische Infrastruktur und die damit verbundenen Anwendungen, die mehr Schwachstellen und Möglichkeiten für Angreifer schaffen. Während sich Analysten über das Ausmaß uneinig sind, sind die meisten überzeugt, dass ein schlecht implementiertes 5G-Netz ein Risiko darstellt. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) nennt zwei Schlüsselaspekte von 5G, die es von früheren Generationen der drahtlosen Telekommunikationstechnologie unterscheiden: *"novel network technologies and concepts - heavily relying on 'softwarisation' and virtualisation of network functions - will introduce new and complex threats."*[29].

Im Vergleich zu 3G- und 4G-Netzwerken **sind 5G-Netzwerke sehr softwareintensiv**, mit Millionen von Codezeilen, die für die Definition, Verwaltung und Verfügbarkeit von Netzwerkfunktionen verantwortlich sind. Das hardwarebasierte Hub-and-Spoke-Switching ist einem dezentralen, softwaredefinierten digitalen Routing gewichen, wodurch Hardware-"Choke-Points", an denen eine Sicherheitsinspektion und -kontrolle

27 Timo Kolb zitiert in Bitkom 2018, S. 45.

28 In Zeiten pandemiebedingter Schließungen sind solche Beeinträchtigungen besonders gravierend, da ein erheblicher Teil der beruflichen Arbeit von zu Hause aus erfolgen muss. Cf. Strand Consult (2020), p.3: „While trade disputes make for sensational news stories, it does not diminish the fact that countries increasingly view telecommunications as vital infrastructure requiring increased security, particularly in light of Covid-19 lockdowns in which people must work, learn, and receive healthcare from home."

29 ENISA (2019), S. 21.

stattfinden könnte, entfallen. Management- und Orchestrierungsfunktionen - einschließlich Sicherheit - werden jetzt fast ausschließlich auf Softwareebene ausgeführt, was sie leichter angreifbar macht. Software für Network Slicing - die dynamische Erstellung und Verwaltung mehrerer virtueller Netzwerke mit unterschiedlichen Eigenschaften - könnte ebenfalls anfällig für Kompromisse sein, da die Cybersicherheitsstandards je nach Anwendungsfall schwanken. Wie die ENISA anmerkt, erfolgt die Virtualisierung von Hardware-Funktionen üblicherweise über Open-Source-Software, -Protokolle und -Systeme - wohlverstandene Werkzeuge, die allen zur Verfügung stehen, auch denjenigen, die Schaden anrichten wollen.[30]

Auch die physische Konfiguration der Infrastruktur bringt Schwachstellen mit sich. Physische Anlagen an der Basis des Netzwerks führen jetzt so viele Aufgaben durch überlagerte Software aus, dass die Anzahl einiger Anlagen reduziert werden kann, was bedeutet, dass ein Verlust in der Servicebereitstellungskette bedeutender wird. Allerdings sind die höherfrequenten Bänder des 5G-Spektrums[31] nur über kürzere Entfernungen als bei 4G verfügbar, was den Bau von wesentlich mehr Zugangspunkten erforderlich macht. Jeder dieser „Zugangsnetzknoten" ist ein weiterer Schwachpunkt, der eine Verbindung zur Kernnetzinfrastruktur herstellt.[32]

Darüber hinaus bedeutet die Verbreitung von Verbindungsgeräten in 5G-Netzwerken, dass die Wahrscheinlichkeit hoch ist, dass unsichere Geräte vorhanden sind, und es unmöglich wird, die Sicherheit aller Geräte zu überwachen. Jedes Gerät wird dann potenziell zu einem Angriffsvektor gegen andere Geräte, oder zumindest für ein isoliertes Segment des Netzwerks. Die Unsicherheiten, die durch Geräte im Internet der Dinge und die mangelnde Absicherung durch ihre Hersteller und Benutzer entstehen, sind gut dokumentiert.[33]

Foto © Stefan Tomic/iStockphoto

30 Basierend auf ENISA (2019), und Wheeler (2019).
31 5G arbeitet auf drei separaten Frequenzbereichen..
32 Basierend auf ENISA (2019), und Wheeler (2019).
33 Basierend auf ENISA (2019), und Wheeler (2019).

4.2 Sicherheit und die Wahl des 5G-Netzwerkausrüsters

Staaten müssen entscheiden, welche Unternehmen sie mit der Installation und Verwaltung von Telekommunikationssystemen betrauen, die für das zukünftige Funktionieren ihres Landes entscheidend sind. Unternehmen agieren immer innerhalb einer staatlichen Gerichtsbarkeit und eines politischen Systems, und nicht alle politischen Systeme stimmen mit den Werten und Zielen westlicher liberaler Gesellschaften überein.

In den letzten Jahren ist das Misstrauen gegenüber chinesischer 5G-Anbieter gewachsen, die unter ihren Konkurrenten das umfangreichste 5G-Infrastrukturangebot haben.[34][35] Der Fall von Huawei wurde am bekanntesten. Chinesische Geräte werden in den USA, Großbritannien, Neuseeland und Australien noch in diesem Jahrzehnt aus den Telekommunikationsnetzen **verbannt**. Deutschland, Frankreich, Italien und Portugal arbeiten an Gesetzen, die von den Regierungen verlangen, sowohl die technische als auch die politische **Zuverlässigkeit von Anbietern** zu berücksichtigen.

Die Technologien und Netzwerke selbst sind zu komplex, als dass die Sicherheitsbehörden den Entscheidungsträgern versichern könnten, dass jede Komponente und jede Zeile des Codes frei von Bugs oder „Hintertüren" für Schwachstellen ist. Sicherheitsbehörden weisen auch darauf hin, dass chinesische Unternehmen der gesetzlich vorgeschriebenen Anforderung, Informationen an die chinesische Regierung weiterzugeben, unterliegen.[36]

Die **Rechtslage** in China zum **Schutz der Privatsphäre** ist sehr vage. Der Begriff „Datenschutz" wurde erst 2009 in die chinesischen Gesetze und Verordnungen aufgenommen, wobei es mehrere rechtliche Möglichkeiten für die Regierung gibt, die Herausgabe von Daten aus dem privaten Sektor anzuordnen.[37] Daher haben chinesische Anbieter nicht einmal eine solide Rechtsgrundlage, um Daten vor der chinesischen Regierung zu schützen.

Wenn man bedenkt, woher vergangene Wirtschaftsspionageakte stammen, könnte man die Sinnhaftigkeit hinterfragen, den **Wolf zum Hirten der Maschinenherde** zu machen. Natürlich kann in einer liberalen Gesellschaft ein Unternehmen nicht mit dem Staat gleichgesetzt werden, aus dem es hervorgegangen ist. Aber in Autokratien ist das anders. Wie der deutsche

Foto © hywards/Shutterstock

34 Lewis (2018), S.4.
35 Crawford (2020).
36 Basierend auf BfV (2019), Watts (2019), Lee (2019).
37 Wang (2017), S. 243.

Inlandsgeheimdienst (BfV) in seinem Jahresbericht deutlich sagt: „Wegen der engen Verflechtung von Staat und Wirtschaft in China ist es im Einzelfall kaum möglich, zwischen staatlich betriebener Wirtschaftsspionage und Ausspähung durch konkurrierende Unternehmen zu unterscheiden."[38]

Das BfV stellt außerdem fest, dass Cyberangriffe auf Deutschland aus China zunehmen. „Als Kernziel kristallisierten sich vornehmlich Wirtschaftsunternehmen heraus. Die Angreifer verfolgen dabei mutmaßlich das Ziel, durch Wirtschaftsspionage und illegitimen Wissenstransfer ausgewählte chinesische Wirtschaftszweige zu fördern und somit insgesamt die chinesischen Ambitionen auf dem Weg zur weltweit führenden Wirtschaftsmacht zu stützen. Den Rahmen für Cyberangriffe setzen unter anderem der aktuelle „Fünf-Jahres-Plan", MIC 2025 sowie die BRI. Die umfangreiche Wirtschaftsspionage und der gezielte, systematische illegitime Wissenstransfer durch chinesische Cyberangriffe richten dabei einen signifikanten Schaden bei betroffenen Unternehmen und der gesamten Volkswirtschaft an."[39]

Die Informationssicherheit als Dreiklang aus Vertraulichkeit, Integrität und Datenverfügbarkeit wird daher schwerlich gewährleistet von 5G-Anbietern aus Rechtssystemen, die den Schutz der Privatsphäre nicht mit der Einschränkung staatlicher Macht verbinden. Der deutsche Sachverständigenrat stellt fest, dass es China an Transparenz in politischen Prozessen mangelt und zudem ein hohes Maß an Korruption herrscht.[40] In einem solchen Umfeld **existiert die Trennung von Markt und Staat nicht**, da sowohl staatliche als auch private Unternehmen privilegierte Beziehungen zur chinesischen Regierung unterhalten müssen, um von wirtschaftlichen Überschüssen zu profitieren.[41] Da 5G Teil einer Debatte über technologische Abhängigkeit und politische Souveränität ist[42], stellt sich die Frage, ob man von Anbietern kaufen sollte, die keiner strikten wirtschaftlichen Logik folgen, sondern von einer autokratischen Regierung abhängig sind.

Es scheint wahrscheinlich, dass chinesische Technologieunternehmen bereits von ihrer Regierung für Hackerangriffe gegen den Westen und die Überwachung von Dissidenten genutzt wurden, insbesondere in Ländern mit schlechter Regierungsführung und schwacher Rechtsstaatlichkeit.[43] Die weltpolitische Lage und die damit verbundenen politischen und wirtschaftlichen Ambitionen Chinas lassen eine weitere Intensivierung der Spionage und Einflussnahme erwarten. Aus unserer Sicht erscheint es naiv anzunehmen, dass die Möglichkeiten, die sich aus dem Zugang zu 5G-Netzen ergeben, ungenutzt blieben.

Wie bereits erwähnt, finanzieren die weltweit führenden Streitkräfte bereits 5G-Technologien für die militärische Nutzung in Stützpunkten, Kommando- und Kontrollarchitekturen und Gefechtsnetzwerken.[44] Regierungen müssen auch bedenken, dass die nationale Sicherheit häufig ein kollektives Unternehmen ist, und dass es notwendig ist, die Sicherheit von 5G jetzt zu berücksichtigen, um zu verhindern, dass später erhebliche (politische und wirtschaftliche) Hindernisse für die bilaterale und multilaterale Zusammenarbeit entstehen. So ist beispielsweise unklar, inwieweit sich nationale Sicherheitsinstitutionen bewusst oder zufällig auf öffentliche 5G-Netze verlassen werden. Die gegenüber europäischen und „Five Eyes"-Verbündeten geäußerten Bedenken der USA beruhen auf dem Argument, dass geteilte Informationen durch nicht-vertrauenswürdige chinesische Anbieter in den zivilen Netzwerken der Verbündeten anfällig für chinesische Spionage sein werden.[45]

Eine frühe Berücksichtigung von Sicherheitsaspekten könnte auch erhebliche Opportunitätskosten innerhalb kollektiver Sicherheitsarchitekturen wie der NATO und der EU verhindern. Bisher gibt es keine einheitliche Herangehensweise an 5G in den Nationen dieser Blöcke. In Erwartung eines solchen „Flickenteppichs" in Europa und anderen Teilen der Welt haben die USA bereits erklärt, dass sie mit Verbündeten und Partnern in einem „Zero-Trust"-Modell arbeiten werden, und treffen die dafür notwendigen industriellen Vorkehrungen.[46]

38 BfV (2019), S. 294.
39 BfV (2019), S. 296.
40 Sachverständigenrat(2016), S. 467.
41 Sachverständigenrat (2016), S. 473.
42 Sachverständigenrat (2019), S. 173.
43 Watts (2019).
44 DoD (2020).
45 FT (2020).
46 DoD (2020).

5 DIE OFFENSICHTLICHEN KOSTEN VON BÖSWILLIGEN NETZWERKAUSRÜSTERN IN 5G-NETZEN

Der Schaden, der durch Angriffe auf Netzwerke zum Stehlen oder Manipulieren von Daten entsteht, ist schwer zu messen. Es gibt mehrere ausgefeilte Ansätze, um den Wert der materiellen und immateriellen Werte zu schätzen, die bei einem solchen Angriff zerstört werden.[47] Einfacher ist es jedoch, den Schaden einer groß angelegten Sabotage des Netzwerks abzuschätzen. Der Ausfall eines Netzwerks ist nicht auf staatlich gesponserte Angriffe beschränkt, sondern kann auch in krimineller Absicht, aus Versehen oder aufgrund von Naturkatastrophen geschehen. Der Verlust von wirtschaftlichen Aktivitäten ist daher gut erforscht. Selbst wenn 5G-Netze noch nicht existieren oder noch nicht die kritischen Funktionen erfüllen, die zuvor beschrieben wurden, kann man vergangene Vorfälle als Analogie dafür verwenden, was ein Ausfall in voller Größe für eine Volkswirtschaft bedeuten könnte (z. B. der Angriff in 2015 bei dem die BlackEnergy Malware auf Unternehmen eingesetzt wurde, die die Stromnetze der Ukraine betreiben[48]).

Die offensichtlichen Kosten von böswilligen - offensichtlich nicht-vertrauenswürdigen - Anbietern lassen sich an folgendem drastischen, aber weniger wahrscheinlichen Szenario verdeutlichen. Wer Zugriff auf das Netzwerk hat und in böswilliger Absicht handelt, kann die 5G-Netzwerke manipulieren. Datengeschwindigkeit oder Latenz können beeinträchtigt werden oder das gesamte Netz kann zum Zusammenbruch gebracht werden.

Nehmen wir also an, dass ein Anbieter nicht vertrauenswürdig ist und unter der Kontrolle einer Regierung steht, die verlangt, einen Kill Switch in europäische 5G-Netzwerke zu integrieren. Auf diese Weise hätte die Regierung ein Werkzeug, das sie in einem politischen Konflikt als Waffe einsetzen kann. Allerdings kann diese Waffe nur einmal eingesetzt werden, denn im Nachgang würde das betroffene Land die Technologie unter der Kontrolle einer solchen feindlichen Regierung mit Sicherheit vollständig ersetzen. Ein solches Szenario ist nicht undenkbar angesichts relativ aktueller Ereignisse wie dem Ransomware-Angriff WannaCry, der Unternehmen auf der ganzen Welt in einer der schwerwiegendsten Hacking-Operationen der Geschichte geschadet hat.[49]

Was China betrifft, so gibt es eine ganze Reihe von Themen, die das Potenzial haben, das Verhältnis zum Westen zu beeinträchtigen, etwa die Souveränität Taiwans, die Internierungslager für Uiguren, die Wasserwege im Südchinesischen Meer oder die Menschenrechte in Hongkong. Sollte es zu einem ernsthaften internationalen Konflikt über diese oder andere Themen kommen, ist es wahrscheinlich, dass die Möglichkeit, sich an der superkritischen Infrastruktur des Gegners zu vergreifen, zu einer politischen Option wird. Im folgenden Abschnitt werden wir uns bemühen, die wirtschaftlichen Auswirkungen eines solchen Angriffs abzuschätzen. Natürlich wäre der politische Effekt, dass eine Regierung nicht handeln kann, wie sie es für richtig hält, weil sie die wirtschaftlichen Folgen oder den Verlust der Souveränität fürchtet, ebenso verheerend.

Angenommen, das zugrundeliegende technische Problem, das ausländischen Akteuren die Manipulation der europäischen 5G-Netze ermöglichte, würde innerhalb weniger Tage behoben werden, so würde es dennoch einen Großteil der - oder gar die gesamte - Wirtschaft lahmlegen. Um die Größenordnung zu verstehen, ist es hilfreich, sich dies anhand eines Zahlenbeispiels vorzustellen.

Jeder Prozentpunkt der jährlichen Arbeitstage kostet nach Angaben der Deutschen Bundesbank etwa 0,3 % des realen Bruttoinlandsprodukts (BIP) in Deutschland.[50] Die Autoren hatten dabei insbesondere Ereignisse wie Feiertage und Brückentage sowie schlechte Witterungsbedingungen im Blick; man kann dies auch auf Zeiten eines Generalstreiks ausweiten.

47 Für mehr Beispiele vgl. https://www.hermeneut.eu/.
48 Cerulus (2019).
49 Greenberg (2017).
50 Deutsche Bundesbank (2012), S.59, und Hansen und Meyer (2018) S.18.

Es ist eine sehr konservative Annahme, dass eine flächendeckende Arbeitsniederlegung durch Sabotage ebenso kostspielig wäre. Im Jahr 2019 betrug das BIP in Deutschland 3,449 Mrd. Euro.[51] Geht man von einem Monat mit 20 Arbeitstagen aus (240 Arbeitstage im Jahr), entspricht ein Prozentpunkt 2,4 Arbeitstagen. Drei Tage Ausfallzeit, z. B. durch einen Kill-Switch-induzierten Kommunikations-Blackout, würden also einer Minderung um 0,375 % des BIP entsprechen, was in absoluten Zahlen etwa 12,94 Mrd. Euro entspricht. Hinzu kämen Kaskadeneffekte in der Folgezeit, einschließlich Folgeschäden, Kosten für vorbeugende Maßnahmen, Austausch defekter Hard- und Software und weiteres.

Wendet man diesen Schätzungsansatz auf zwei der drei anderen Länder an, die wir in unseren Länderstudien weiter unten und in separaten Dokumenten behandeln - nämlich Frankreich und Italien -, und fügt Berechnungen hinzu, die auf Zahlen des portugiesischen Finanzministeriums beruhen, erhält man für diese Länder ungefähre Zahlen (siehe Tabelle 5).

Tabelle 5: Geschätzte Kosten eines Totalausfalls des Kommunikationsnetzes

Kosten eines Totalausfalls von X Tagen, in Milliarden Euro			
	1 Tag	3 Tage	6 Tage
Frankreich	2,788	8,363	16,727
Deutschland	4,313	12,940	25,880
Italien	2,057	6,171	12,342
Portugal	0,425	1,275	2,549

Quelle: eigene Berechnungen, basierend auf Daten der Weltbank[52], Bundesbank[53] und dem Portugiesischen Finanzministerium[54].

Nicht alle Sektoren der Wirtschaft wären in gleicher Weise betroffen, und einige könnten sich als widerstandsfähiger erweisen und in der Lage sein, die entgangene Produktion aufzuholen. Während es für Unternehmen, die mit Akkordarbeit arbeiten, nahezu unmöglich sein wird, ungeplante Ausfallzeiten zu kompensieren, hängt die Gesamtwirkung auf die Wirtschaft von ihrem Grad an gegenseitiger Abhängigkeit ab, wobei sich die Sektoren gegenseitig beeinflussen und es zu Kaskadeneffekten kommt. Auf kurze Unterbrechungen könnten zwar Versuche folgen, den Rückstand aufzuholen, die deutsche Bundesbank gibt jedoch an, dass sich solche Versuche nicht genau quantifizieren lassen[55]. Das portugiesische Finanzministerium schätzt, dass die Kosten einer längeren Unterbrechung jedoch überproportional anfallen.[56]

Neben dem unwahrscheinlichen Kill-Switch-Szenario ist ein weitaus realistisches, aber weniger bekanntes „Worst-Case-Szenario" denkbar. Der Betrieb, die Verwaltung und die Wartung von 5G-Netzen werden in hohem Maße von der Anwendung künstlicher Intelligenz abhängen (Details siehe Abschnitt *Künstliche Intelligenz in 5G-Netzwerken* unten). Die KI-Algorithmen können von böswilligen Akteuren manipuliert werden, mit schwerwiegenden, aber weniger sichtbaren Folgen.

51 Statistisches Bundesamt (2020).
52 World Bank (2020).
53 Deutsche Bundesbank (2012).
54 Jornaldenegocios (2020).
55 Deutsche Bundesbank (2012).
56 Jornaldenegocios (2020).

6 DIE VERSTECKTEN KOSTEN VON NICHT-VERTRAUENSWÜRDIGEN NETZWERKAUSRÜSTERN IN 5G-NETZEN

Neben den offensichtlichen Kosten, die entstehen, wenn ein superkritisches 5G-Netz sabotiert wird, gibt es auch weniger sichtbare oder versteckte Kosten, die entstehen, wenn die Vertraulichkeit und Integrität des Netzes und seiner Daten beeinträchtigt wird. Diese Kosten sind versteckt, weil sie entweder zu einem späteren Zeitpunkt auftreten oder weil sie von anderen Personen oder Institutionen getragen werden als denen, die über die Architektur eines 5G-Netzwerks entscheiden. Für die Gesellschaft als Ganzes sind all diese Kosten jedoch relevant und müssen bei der Entscheidung, wem man mit dem Aufbau der Netzinfrastruktur der nächsten Generation beauftragt, berücksichtigt werden.

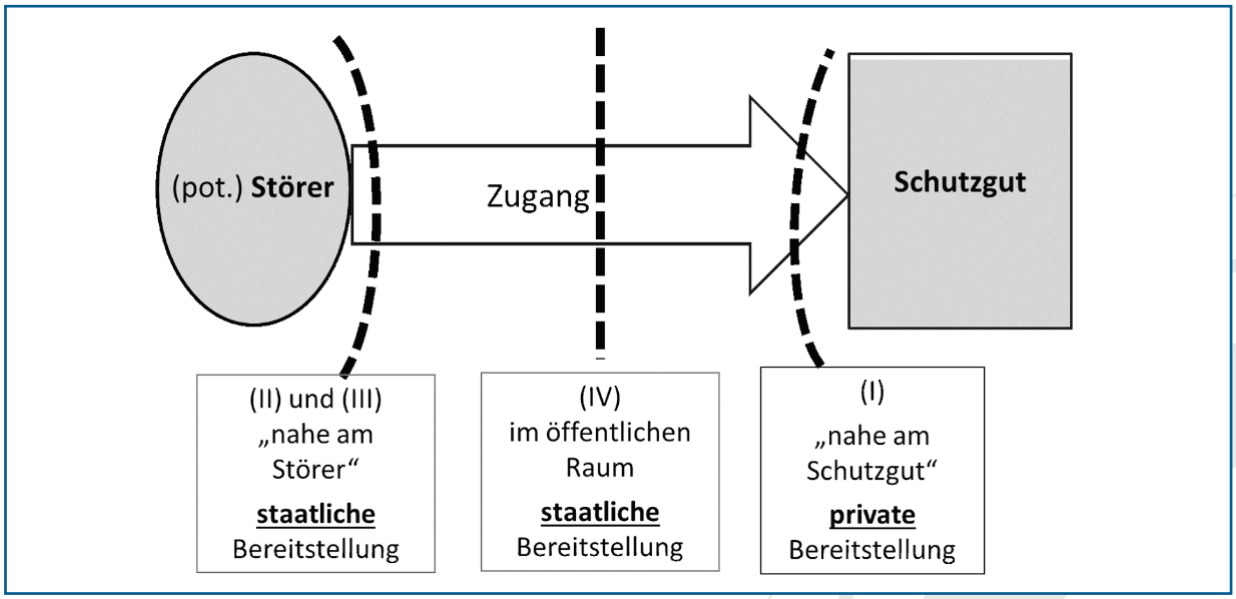
Im folgenden Abschnitt versuchen wir, diese versteckten Kosten aufzudecken, sie zu definieren und in einigen Fällen einen Ansatz zur Messung zu finden. Letzteres ist oft schwierig oder sogar unmöglich, da uns die notwendigen Daten fehlen, aber es wird deutlich werden, dass es nicht ausreicht, die Angebote der fünf Netzwerkanbieter für die Hard- und Software (und manchmal auch für das Management) zum Aufbau des Netzwerks zu vergleichen. Stattdessen sind die Kosten für die gesamte Volkswirtschaft über den Lebenszyklus des Netzes relevant, wenn es um die Entscheidung geht, an wen der Auftrag zum Aufbau eines 5G-Netzes vergeben werden soll.

6.1 Der ökonomische Charakter von Sicherheit

Eine Weigerung des Staates und der Mobilfunkanbieter, nur vertrauenswürdige Anbieter für den Aufbau von 5G-Netzen einzusetzen, würde die Kosten für den Schutz auf Unternehmen (insbesondere sicherheitssensible) und Bürger verlagern. Laut Bretschneider et.al. (2020) wäre es Aufgabe des Staates, präventiv und nah am Angreifer einzugreifen[57].

Schutzleistungen haben hier eher den Charakter eines öffentlichen Gutes. Die Weigerung des Staates, diese Aufgabe wahrzunehmen, verlagert die Kosten und den Handlungsbedarf auf den Eigentümer des schutzbedürftigen Gutes (siehe Abb. 2: Staatliche und private Bereitstellung von Sicherheit).

Abbildung 2: Staatliche und private Bereitstellung von Sicherheit.



Quelle: Bretschneider et. al. (2020), S. 106.

57 Bretschneider et.al. (2020), S. 106 Abb. 2.

Man könnte auch argumentieren, dass Maßnahmen zum Schutz des gesamten Netzwerks billiger sind, als diese zu kompensieren, indem jeder einzelne an das Netzwerk angeschlossene Mobilfunkkunde geschützt werden muss. Schließlich sind es deren Daten, hinter denen Länder wie China her sind. Oder, wie es Bitkom formuliert: *„in the economic environment, sabotage, espionage and data theft are aimed at digital data or the information and communication infrastructure of industrial companies. Advanced digitisation makes it increasingly easy for criminals to gain access to this data"*.[58]

Oder, ökonomischer ausgedrückt: **Die Digitalisierung senkt die Kosten für den Angreifer** für Sabotage und Datendiebstahl, wodurch die „Rentabilität" steigt, die Eintrittsbarriere für Angreifer sinkt und die Angebotskurve für Angriffe sich nach rechts verschiebt (siehe Abb. 2). Ohne zusätzliche Anstrengungen, diesem Trend entgegenzuwirken, werden wir mit mehr erfolgreichen Angriffen und höheren Verlusten für Unternehmen und Bürger rechnen müssen. Mit der Verfügbarkeit von 5G (und, noch wichtiger, den darauf basierenden Anwendungen) wird sich dieser Trend nur weiter verstärken.

Schon jetzt mangelt es KMUs an ausreichender IT- und Datensicherheit, da die Kosten für den Schutz hohen Skaleneffekten sowie positiven externen Effekten unterliegen.[59] Zudem sind KMU in ihrer Wertschöpfungskette tendenziell weniger digitalisiert. Ein Grund dafür ist das mangelnde Vertrauen in die Sicherheit der Anbindung der Produktion an das Internet. Folglich nutzen KMU weniger häufig Cloud Computing. Es ist davon auszugehen, dass sich dieses Muster auch bei der Nutzung der mit 5G verbundenen Möglichkeiten zeigen wird.

Sicherheits- und Digitalexperten, aber auch Politiker sprechen immer wieder von einem **„Security by Design"** anstelle eines **„Funktionalität zuerst, Cybersicherheit später"**-Ansatzes. Der Beginn einer Technologieimplementierung ist der Zeitpunkt an dem entschieden wird, ob wir wieder die gleichen Fehler machen wie beim Aufbau des allgemeinen Internets: Wir bauen ein Kommunikationsnetz, an das wir entscheidende Teile unserer Wirtschaft anschließen und dadurch an Produktivität gewinnen, bis dieses Netz für kriminelle oder andere Aktivitäten missbraucht wird. Erst wenn solche Schäden auftreten, wird der Schutz eines inhärent unsicheren Netzwerks wichtig.[60] Natürlich wird die **Verwendung von nur vertrauenswürdigen Anbietern** in 5G-Netzwerken nicht ausreichen, um die Sicherheit eines Netzwerks zu garantieren, aber es verringert die Wahrscheinlichkeit von Angriffen durch mögliche Opponenten.

Bitkom behauptet, dass bereits 18 % aller Cyberangriffe auf deutsche Unternehmen aus China kommen.[61] Es braucht nicht viel Weitsicht, um vorherzusagen, dass, **wenn der Angriffsvektor zunimmt,** weil zahlreiche lohnenswerte Ziele mit dem Netz verbunden sind, auch **die Zahl der Angriffe steigen wird**. Es scheint ebenso offensichtlich, dass, wenn der Angriffsvektor in China hergestellt wird, der Anteil der Angriffe, die aus China stammen, steigen wird.

Sicherheit hat ihren Preis. Die Gefahr der wirtschaftlichen und politischen Ausbeutung durch einen Gegner muss durch entsprechende Schutzmaßnahmen kompensiert werden. Diese Maßnahmen erfordern Ressourcen und Ressourcen kosten Geld. Eine intuitive Annäherung zu diesem Themenkomplex ist die Beschreibung verschiedener Kontrollmechanismen. Hier kann man zwischen präventiven, reaktiven und aufdeckenden Kontrollmaßnahmen unterscheiden. Die zugrundeliegende Idee ist, dass all diese Aktivitäten – teilweise oder vollständig – durchgeführt werden müssen, weil ein oder mehrere nicht-vertrauenswürdige Anbieter am Kommunikationsnetzwerk teilhaben.

Präventive Maßnahmen werden zeitlich vor dem Auftreten eines unerwünschten Ereignisses durchgeführt, um potenzielle Gefahren für die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu reduzieren. Um einen Angriff zu verhindern, werden Ressourcen eingesetzt, die es dem Angreifer erschweren, den Angriff durchzuführen. Oder, im Extremfall, wird ein Angriff verhindert, indem man sich dem Risiko überhaupt nicht aussetzt. In unserem Fall würde dies bedeuten, sich nicht mit einem Netzwerk zu verbinden, dass vertrauensunwürdige Komponenten enthält.

58 Bitkom (2018), S. 16.
59 Park et al. (2008), S. 92.
60 Herpig (2020), S. 2.
61 Bitkom (2018), S. 29.

Erkennungsmaßnahmen sind fortlaufende, routinemäßige Verfahren, die es ermöglichen, Anomalien und Angriffe frühzeitig zu entdecken, um das Ausmaß des Schadens zu reduzieren. Sie können den Betrieb von Sensoren und Security Operations Centers (SOC) sowie die Überprüfung von Codezeilen in Software-Patches umfassen.

Reaktive Maßnahmen sind Schritte zur Schadensbegrenzung, die im Anschluss an einen Vorfall ergriffen werden. Sobald ein Angriff entdeckt wird, müssen der Netzbetreiber und die betroffenen Kunden das Ausmaß des Schadens begrenzen und sicherstellen, dass sich ein ähnlicher Angriff nicht wiederholen kann. Dazu kann auch der Austausch bestimmter Technik oder Software im Netz gehören, was im schlimmsten Fall eine vorübergehende Abschaltung des gesamten Dienstes beinhalten kann. Für die Netzkunden gibt es auch die Möglichkeit, ihr Geschäft zu vertrauenswürdigen Netzbetreibern zu verlagern, wie es nach den Snowden-Enthüllungen zu beobachten war.

6.2 Prävention und Kontrolle

Wie bereits erwähnt, erfordert ein Mangel an Vertrauen in die Integrität und Verfügbarkeit eines Netzwerks zusätzliche Maßnahmen, um Verlässlichkeit in der Funktionalität des Netzwerkes sicherzustellen. Diese Maßnahmen können technischer Art sein (eine Lösung, die die Vertraulichkeit, Integrität und Verfügbarkeit von Daten in einem inhärent unsicheren Netzwerk ermöglicht) oder verwaltungstechnischer Art sein (verschiedene Formen des Risikomanagements).

Eine weitere Möglichkeit, solche Kontrollen - die im Grunde genommen abmildernde Maßnahmen zu verschiedenen Zeitpunkten sind - zu betrachten, findet sich in der Toolbox der Europäischen Union für risikomindernde Maßnahmen, die sich auf die Cybersicherheit von 5G-Netzen bezieht. Sie unterscheidet zur Eindämmung von Risiken strategische, technische und unterstützende Maßnahmen.[62]

Strategische Maßnahmen umfassen Aspekte der Regulierung und Versorgung. Technische Maßnahmen beziehen sich auf grundlegende und spezifische Netzsicherheitsvorkehrungen, Anforderungen an die Bereitstellung von Diensten und Produkten, Ausfallsicherheit und Vorkehrungen, die die Kontinuität im Falle eines glaubwürdigen Notfalls ermöglichen. Unterstützende Aktivitäten erhöhen die Effektivität von Maßnahmen beider Typen.

Die Toolbox ist bereits in vollem Umfang verfügbar und die Europäische Kommission hat mit den Mitgliedsstaaten zusammengearbeitet, um den Fortschritt ihrer Implementierungen zu verfolgen. Während beispielsweise der Bereich der regulatorischen Eingriffe so ausgereift ist, dass diese positiv bewertet wurden, werden andere, wie die Diversifizierung der Versorgung und technische Maßnahmen, immer noch als risikobehaftet angesehen. Dies zeigt, wie wichtig es ist, Anbieterstrategien zu entwerfen, die die nationalen und europäischen Interessen schützen, und diese durchzusetzen, sowie sich gegen die unbekannten Kosten abzusichern, die entstehen, wenn man diesen Anbietern erlaubt, Teil des 5G-Netzes zu sein.

Darüber hinaus sind die **Prague Proposals** von Interesse. Diese wurden auf der Prager 5G-Sicherheitskonferenz am 3. Mai 2019 vorgeschlagen. Sie sind in vier Kategorien eingeteilt: Politik, Technologie, Wirtschaft und der Nexus von Sicherheit, Datenschutz und Resilienz.[63] Diese Entwürfe sind zwar nicht verbindlich, bilden aber das Rückgrat der nachfolgenden Diskussionen und Verpflichtungen der teilnehmenden Länder, die jeweils ihre Strategien im Hinblick auf die Versteigerung von Frequenzen und den Ausbau ihrer Netzsicherheit anpassen, um auf diese Anforderungen zu reagieren.

6.2.1 Technologie

Die Technologie zum Schutz eines Netzwerks, in dessen Aufbau nicht-vertrauenswürdige Anbieter involviert sind, muss garantieren und sicherstellen, dass bestehende und neue Systeme angemessene Zugriffskontrollrichtlinien festlegen und den Zugriff durch Dritte einschränken. Zudem muss sichergestellt werden, dass, wenn ein Fernzugriff erforderlich ist, eine Zero-Trust-Authentifizierung, d.h. eine

62 Für mehr Infos zur Toolbox der EU siehe DG Connect (2020).
63 Prague Proposals (2019).

Foto © gorodenkoff/iStockphoto

Autorisierung und Protokollierung auf Subsysteme, angewendet wird, um zu gewährleisten, dass stets ein Überblick über den Zugriff auf Daten und durchgeführte Änderungen besteht. Der Einsatz von VPNs und insbesondere von Zero-Trust-Modellen muss über die gesamte Netzwerkinfrastruktur, die Verwaltungsfunktionen und den softwaredefinierten Betrieb hinweg so erfolgen, dass der Zugriff und die Verwaltung auf Subsysteme beschränkt sind, dass der Fernzugriff keinen breiten Zugriff auf Geräte und Dienste impliziert und dass eine strikte Identität für Subsysteme gewährleistet ist.

Diese Subsysteme müssen auch entsprechend isoliert werden, so dass der Zugriff auf unkritische Systeme in diesem Modell keinen Zugriff auf andere (kritischere) Subsysteme ermöglicht. Dies bedeutet, dass die Kosten für jedes neue Stück Infrastruktur (Small Cell, Edge-Netzinfrastruktur und zugehörige Software) steigen, da nicht nur der Zugang gesichert werden muss. Die zugehörige Firmware, die Hardware-Zugriffsfunktionen und die Virtualisierung müssen gesichert und standardisiert werden, um zu gewährleisten, dass herstellerspezifische Implementierungen die Vertrauensversprechen auf jeder Stufe einhalten. **Network Operation Centres (NOC) und Security Operation Centres (SOC) müssen für Mobilfunknetzbetreiber vor Ort** und innerhalb von Ländern, in denen demokratische Institutionen und ordnungsgemäße Verfahren angewendet **werden, betrieben werden.**

Die überwiegende Mehrheit der Betreiber (75%) gab in einer Studie aus dem Jahr 2017 an, dass **Komplexität und Kosten die Implementierung von fortschrittlichem Signalisierungsschutz blockieren.** Selbst Technologie-Stacks mit offener Spezifikation wie OpenSS7, die potenziell geringere Installations- und Testkosten verursachen, werden nur begrenzt angenommen, da sich kommerzielle Unternehmen, die das Netzwerk betreiben, auf die wertschöpfenden High-Level-Komponenten des Stacks konzentrieren und nicht auf die zugrundeliegenden Protokolle. Dieses Risiko setzt die besagten High-Level-Komponenten versteckten Bedrohungen aus, die von böswilligen Anbietern ausgenutzt werden können.[64]

64 ENISA (2018), ITU (2019).

Darüber hinaus wird die Beteiligung von nicht-vertrauenswürdigen Anbietern die Einführung von Schutzlösungen und -technologien beschleunigen und ausweiten, insbesondere die **Ende-zu-Ende-Datenverschlüsselung.** Während die direkten Kosten einer solchen Schutzmaßnahme in Bezug auf die Infrastruktur sinken, sind die indirekten Kosten aufgrund erhöhter Latenz schwer abzuschätzen, da sie von mehreren Parametern wie dem Dienst, dem Protokoll und dem Verschlüsselungsschema abhängen. Wie im Whitepaper der 5G PPP Security WG hervorgehoben wird, *"… End-to-end encryption may hamper the use of multiple value-added security services such as attack detection, QoS monitoring, fine-grained access control, among others …"* [65]. Generell hat die Verwendung von Verschlüsselung mehrere Nachteile, die bei einem großflächigen Einsatz kostspielig sein können.

Selbst wenn die Verschlüsselung flächendeckend eingeführt wird, bleibt das Problem der **Sicherheit der Metadaten** bestehen. Während die Nutzdaten verschlüsselt und damit für unbefugte Dritte unlesbar gemacht werden können, bleiben Informationen darüber, wer mit wem zu welchem Zeitpunkt kommuniziert, sichtbar, da Netzwerke diese Informationen für Routing- und Abrechnungszwecke verwenden. Dieses Metadatenleck kann sehr aufschlussreich sein; es würde z. B. detaillierte Einblicke in die Häufigkeit und Intensität von Geschäftsbeziehungen zwischen Organisationen geben. Diese könnten für Börsenmanipulationen und Insiderhandel, sowie anstehende Handelsgeschäfte genutzt werden oder Kommunikationspartner geschützter Berufsgruppen offenbaren, um nur einige Beispiele zu nennen. Ein nicht-vertrauenswürdiger Anbieter hätte über seine Hardware Zugriff auf diese Metadaten-Informationen und könnte sie zu seinem wirtschaftlichen oder politischen Vorteil nutzen.

Die oben genannten Faktoren verstärken nur die Argumentation für eine Ende-zu-Ende-Verschlüsselung und Zero-Trust-Sicherheitsarchitekturen, die die Daten und Metadaten der Endnutzer schützen sowie den Zugang zu kritischen oder weichen Zielen des gesamten 5G-Netzwerks sichern und isolieren. Schließlich müssen auch zusätzliche Sicherheitsmaßnahmen ergriffen werden, um die physischen Zugänge zur Infrastruktur zu sichern, damit diese kontrolliert werden können. Diese physischen Sicherheitsmaßnahmen sind jedoch unabhängig von der Vertrauenswürdigkeit des Anbieters.

6.2.2 Cyberbedrohungsanalyse

Wenn nicht-vertrauenswürdige Technik ein integraler Bestandteil eines Netzwerks innerhalb von Netzwerken ist, wird dieses mit potenziell mehr Schwachstellen konfrontiert und stellt damit ein größeres Risiko für Regierungen, Unternehmen und Bürger dar. Die geringere Sicherheit eines solchen Netzwerks kann zumindest teilweise dadurch kompensiert werden, dass man mehr Aufwand und Geld in die Überwachung und Kontrolle des nicht-vertrauenswürdigen Netzwerks gesteckt wird. Dazu wird folgendes benötigt:

1. Eine bessere **Übersicht** über das, was im Netzwerk passiert,

2. einen **Prüfstand**, um herauszufinden, was in und mit einem nicht-vertrauenswürdigen Netzwerk passieren könnte,

3. ein institutionelles Arrangement zum **Austausch von Informationen** zwischen konkurrierenden Netzwerkbetreibern und mit der nationalen Cybersicherheitsbehörde.

4. ein institutionelles Arrangement zum Austausch von Informationen innerhalb der EU und mit gleichgesinnten Staaten.

Ein **nationales Informationsaustausch- und Analysezentrum** für 5G-Netze wird ohnehin benötigt, auch wenn die Netze nur vertrauenswürdige Technik enthalten werden. Bugs und Exploits wird es immer geben. Darüber hinaus muss jedoch ein Austauschmechanismus eingerichtet werden, über den sich Betreiber und Kunden gegenseitig über verdächtige Aktivitäten in nicht-vertrauenswürdigen Netzen informieren können. Während bei vertrauenswürdigen Anbietern ein gemeinsames Interesse daran besteht, das Netzwerk sicher zu halten, wird bei vertrauensunwürdigen Anbietern genau dies in Frage gestellt und es muss daher sorgfältig abgewogen werden, ob der Anbieter in diesem Fall in den Kreis des Vertrauens gezogen werden kann, in dem sensible Informationen ausgetauscht werden.

65 5G PPP Security WG.

Der Informationsaustausch ist entscheidend, um die Informationskosten für jeden Marktteilnehmer zu reduzieren und um sicherzustellen, dass sich ein Angriffsmuster nicht wiederholen kann. Aus früheren Versuchen, Informationen über Cybersicherheitsvorfälle bei Anbietern kritischer Infrastrukturen zu teilen, wissen wir jedoch, dass private Unternehmen zögern, solche Informationen mit Konkurrenten oder der Regierung zu teilen, aus Sorge vor negativen Marktreaktionen.

Über das Wissen hinaus, was in einem Netzwerk vor sich geht, ist es auch wichtig zu wissen, was vor sich gehen könnte. Insbesondere Netzwerke mit nicht-vertrauenswürdiger Technologie müssen ständig auf Schwachstellen oder bösartige Tools getestet werden, die einem Angreifer Zugang zu einem Netzwerk verschaffen. In einem unabhängigen **5G-Testzentrum** kann ein digitaler Zwilling des nicht-vertrauenswürdigen Netzwerks unter Laborbedingungen getestet werden. White-Hat-Hacker können nach Schlupflöchern und Möglichkeiten suchen, die Kontrolle über das Netzwerk zu übernehmen oder einen Teil der Daten heimlich abzuleiten.

Die **nationale Cybersicherheitsbehörde** muss die Schwachstellen von 5G-Netzwerken aufzeichnen und diese mit den Bedrohungsinformationen spiegeln, die sie aus ihren eigenen Analysen oder von Partner-Nachrichtendiensten erhält. All diese nationalen Bemühungen müssen sich auch auf EU-Ebene widerspiegeln, zum Beispiel bei ENISA, um von den Erfahrungen und dem Wissen gleichgesinnter Länder zu lernen.

6.2.3 Prüfzentrum für 5G-Netzwerke und Anwendungen mit nicht-vertrauenswürdiger Technologie

Die Entwicklung von 5G-Netzen ist noch nicht abgeschlossen. Zukünftige Upgrades werden die Netze in die Lage versetzen, noch mehr Funktionen zu erfüllen, und damit neue Geschäftsmodelle ermöglichen. Für die Verbesserung der 5G-Netze und für die Entwicklung von Anwendungen ist noch viel Forschungs- und Entwicklungsarbeit zu leisten. Hierfür sind F&E-Labore und Prüfstände eine notwendige Infrastruktur.

Solche Labore und Prüfstände werden auch benötigt, um mehr über die Schwachstellen von Netzwerken, insbesondere von solchen, die nicht-vertrauenswürdige Technologie enthalten, zu erfahren. Während die britische Regierung technische Tests durchführen ließ, die ihr bei der Entscheidungsfindung der Vertrauenswürdigkeit chinesischer 5G Technologie helfen sollte, wurde deutlich, wie viele Ressourcen für dieses Unterfangen benötigt werden. Daher empfahl das National Cyber Security Centre des Vereinigten Königreichs die Einrichtung eines **National Telecoms Lab**, das Netzwerke unter verschiedenen Bedingungen und mit einer Variation von Herstellertechnik testen könnte.[66]

Um die Kosten für ein solches Testzentrum zu kalkulieren, kann man mit einem **Top-Down-Ansatz** nach Analogien suchen, die bereits existieren. Ein aktuelles Beispiel ist das Fraunhofer-Institut für Integrierte Schaltungen, das im Rahmen der 5G-Bayern-Initiative den Zuschlag für einen Prüfstand erhalten hat. Als Anfangsfinanzierung erhielten sie vom Wirtschaftsministerium einen Zuschuss von mehr als 25 Mio. Euro.[67] Um ein solches spezialisiertes angewandtes Forschungsinstitut zu betreiben, ist mehr Unterstützung nötig.

Das Personal, das erforderlich ist, um die Sicherheit der in Frankreich implementierten Telekommunikationsgeräte in zufriedenstellender Weise zu prüfen und zu kontrollieren, kann auf mindestens 150 multidisziplinäre Experten geschätzt werden: hochrangige Ingenieure und Juristen, die Handelsverträge prüfen und verifizieren, ob die von ausländischen Lieferanten gelieferten technischen Übersetzungen richtig und realitätsgetreu sind, und die entsprechende Rechtstexte vorbereiten. Die gesamte wünschenswerte Lohnsumme tendiert daher zu einer ungefähren und minimalen Spanne von 12 bis 16 Mio. Euro pro Jahr, zu der noch die Betriebskosten hinzugezählt werden müssen. Unter Berücksichtigung der umfangreichen technischen Mittel, die für eine solche Mission bereitgestellt werden müssen (Labor, Prüfstände etc.), kann das Gesamtbudget im Falle eines nicht-vertrauenswürdigen Telekommunikationsanbieters mit etwa 30 Mio. Euro pro Jahr veranschlagt werden.

Natürlich gibt es Forschungsinstitute in verschiedenen Größen, je nach Umfang der Themen, an denen sie

66 NCSC (2020), S. 25.
67 Fraunhofer IIS (2020).

arbeiten. Da wir selbst aus solchen Forschungsinstituten kommen, halten wir es für realistisch und notwendig, dass ein nationales Institut sich vollständig der 5G-Netzsicherheit widmet, die Software von nicht-vertrauenswürdigen Anbietern über die Lebensdauer eines 5G-Netzes testet und verifiziert. Ein praktikabler **Vergleichswert**, der diese Größenordnungen bestätigt: Das Forschungszentrum **IRT-SystemX**, das sich auf die Analyse des Bedarfs an digitaler Sicherheit in Bezug auf das Internet der Dinge, kommunizierende Fahrzeuge und Industrie 4.0 konzentriert, ist mit einem Personalbestand von 140 Personen - hauptsächlich Forschern - und einem Budget von 23 Mio. pro Jahr dimensioniert. Je nach Größe der Wirtschaft wird der Betrag natürlich variieren.

Ein alternativer **Bottom-up-Ansatz** zur Berechnung der Kosten für das Testen und Verifizieren der Vertrauenswürdigkeit einer Software und des Netzwerks besteht in der Abschätzung der Kosten für eine **Quellcodeüberprüfung**. White-Box-Tests eines Produkts auf der Grundlage einer Quellcodeüberprüfung sind eine gängige Methode für Produkte mit einer starken Verbindung zur Sicherheit, und eine Vielzahl von Anbietern bietet Regierungen und unabhängigen Prüfern die Möglichkeit, den Quellcode ihrer Produkte als vertrauensbildende Maßnahme zu bewerten. Ein bedeutendes und gängiges Beispiel hierfür ist das Government Security Program von Microsoft.[68] Im folgenden Abschnitt werden wir die potenziellen Kosten einer solchen Quellcodeüberprüfung im Falle von 5G abschätzen.

Einfach ausgedrückt sind die **Auditkosten** eine Funktion des Produktumfangs, der Geschwindigkeit, mit der es auditiert werden kann, und der damit verbundenen Kosten für den Auditprozess selbst sowie des organisatorischen Aufwands. Die Funktionalität eines Produkts wird sowohl durch Software als auch durch Hardware bereitgestellt, die unterschiedliche Audit-Ansätze erfordern, wobei die Komplexität der ersteren typischerweise in Metriken wie Quellcodezeilen (Source Lines of Code – SLOC) gemessen wird. Die Kosten für ein Software-Code-Audit können daher näherungsweise wie folgt berechnet werden:

product SLOC * avg. SLOC review capability / hour * auditor cost / hour.

Dies liefert eine Obergrenze für die Kosten einer Softwareüberprüfung, da nicht alle Teile einer Software in Bezug auf die Sicherheit gleich wichtig sind. Betrachten wir den Fall eines Betriebssystems, das z. B. Funktionen zur Anzeige von Inhalten auf dem Bildschirm, zum Empfang von Benutzereingaben

Foto © 512r/Shutterstock

68 Für mehr Informationen vgl. https://www.microsoft.com/en-us/securityengineering/gsp.

über Maus und Tastatur, zur Kommunikation über das Netzwerk und zur Verwaltung von Benutzer- und Dateiberechtigungen umfasst. Wenn ein Hersteller die Absicht hat, die Kontrolle über Geräte zu übernehmen, würden sich einige Stellen, wie z. B. der Softwarecode für die Benutzerverwaltung oder die Dateiberechtigungen, als erstklassige Ziele für eine solche Hintertür anbieten, während andere nur einen begrenzten Nutzen für einen Angreifer bieten würden. Die gleiche Argumentation gilt auch für 5G, das viele Funktionen enthält, zum Beispiel für die Verwaltung der Funkschnittstelle oder die Signalverarbeitung. Für eine praktischere Schätzung der Auditing-Kosten würde die obige Berechnung daher um den Anteil des Produkts mit direkten Sicherheitsauswirkungen reduziert, der je nach Art der Komponente zwischen 15 und 30 % liegen könnte.

Es gibt mehrere Datenpunkte zur Annäherung an die Softwarekomplexität von 5G Radio-Access- Network-Komponenten. Die neueste Version der herstellerneutralen Open-Source-Implementierung OpenRAN vom Juni 2020 enthält insgesamt 1.089.389 SLOC, während der kommerzielle Anbieter Ericsson angab, dass *"the software complexity of [their] RAN in a baseband exceeds that of Boeing 787 aircraft."*[69], was eine untere Grenze von 6,5 Mio. Quellcodezeilen setzen würde.[70] Zusätzliche Ausgaben müssten für die Überprüfung der Firmware des eingebetteten Systems, des Mikrocodes des Chipsatzes[71] und die Verifizierung der Hardware-Designs eingeplant werden.

Die wissenschaftliche Literatur zur **Effizienz von Quellcode-Reviews** ist spärlich, aber eine Studie eines Anbieters von Software-Engineering-Toolkits ergab, dass in der Praxis eine Code-Review-Leistung von bis zu 500 SLOC pro Stunde erreicht werden kann, über die hinaus die Effizienz bei der Fehlererkennung deutlich abnimmt.[72]

Für eine Berechnung des Nutzens würden wir ein durchschnittliches Gehalt für einen sicherheitsgeschulten Software-Ingenieur von 125.000 Euro pro Jahr annehmen und das Standardverfahren für Gemeinkosten in Höhe von 25 % anwenden, das bei Zuschüssen der Europäischen Union angewendet wird. Basierend auf 1600 Arbeitsstunden pro Jahr könnte die Obergrenze für ein Software-Audit der OpenRAN-Implementierung auf 212.500 Euro geschätzt werden, während das entsprechende kommerzielle Produkt von Ericsson mit 1,25 Mio. Euro für eine Quellcode-Überprüfung zu Buche schlagen würde. Die Zahl könnte, wie oben diskutiert, reduziert werden, wenn nur ausgewählte Teile des Codes inspiziert werden müssten.

Es gibt jedoch zusätzliche Aspekte, die möglicherweise berücksichtigt werden müssen. Da es sich um eine neue Technologie und ein größtenteils softwarebasiertes Produkt handelt, ist zu erwarten, dass die Hersteller nach dem ersten Einsatz des Produkts **in regelmäßiger Folge** neue Produktfunktionen herausbringen und Fehlerkorrekturen sowie **Software-Updates** herausgeben werden. Daher müsste der Quellcode-Audit wiederholt durchgeführt werden, um auch die Sicherheit zukünftiger Änderungen zu gewährleisten. Auch wenn solche Änderungen regelmäßig auftreten, würde der Großteil des Produkts unverändert bleiben, was auch bedeutet, dass der Großteil der Auditkosten im Voraus anfällt, während Updates zu einem Bruchteil des ursprünglichen Preises bewertet werden können.

Die Prüfung des Quellcodes des Produkts ist jedoch nur ein Teil des Verfahrens, um eine sichere 5G-Bereitstellung zu gewährleisten. Die Audit-Verfahren müssen in hohem Maße in den Produktaufbau integriert werden, um sicherzustellen, dass der überprüfte Quellcode tatsächlich die gleiche Software ist, die an die im Feld installierten Geräte geliefert wird. Dies erfordert Absprachen mit dem Produkthersteller und zusätzliche Prozesse auf Kundenseite, um **die Lieferkette zu kontrollieren und zu auditieren**, was weitere Kosten verursacht.

6.2.4 Künstliche Intelligenz in 5G-Netzen

Künstliche Intelligenz (KI) hat sich in verschiedenen Anwendungsbereichen als praktikable und effektive Lösung erwiesen und ist ein Enabler für die Bereitstellung von 5G-Netzwerken. Es wurde besonders darauf geachtet, dass sich die Mobilfunkbetreiber

69 Ericsson (2020c).
70 Information is beautiful (2020).
71 Chips, Prozessor- und Speicherhardware können durch verschiedene Hintertüren so manipuliert werden, dass sie Remote-Befehle von fremden Entitäten empfangen: Software-Dienste auf höherer Ebene können streng geprüft werden, sind aber auf niedrigere Schichten angewiesen, die nicht unbedingt geprüft werden.
72 Smartbear (2019).

der Sicherheitsrisiken im Zusammenhang mit 5G bewusst sind. Da es sich bei 5G um eine aufstrebende Technologie handelt, ist eine Bewertung der Kosten zur Vermeidung oder Abschwächung dieser Risiken derzeit nicht möglich. Daher haben die nächsten Unterabschnitte im Gegensatz zum Rest dieses Strategiepapiers in erster Linie das Ziel, ein Bewusstsein für die potenziellen (versteckten) Kosten der Annahme eines nicht-vertrauenswürdigen Anbieters zu schaffen.

Gründe für KI in 5G-Netzen und damit verbundene Kosten

KI ist die Simulation von menschlichen Intelligenzprozessen durch Maschinen. KI-Programme konzentrieren sich auf drei primäre kognitive Fähigkeiten:

- **Lernen**, auch Training genannt (Erfassen von Daten und Erstellen von Regeln zum Sortieren dieser Daten),
- **Schlussfolgern** (Auswahl der richtigen Daten, um das gewünschte Ergebnis zu erzielen) und
- **Selbstkorrektur** (Feinabstimmung der Datensortierung für möglichst genaue Ergebnisse).

Für solche Fähigkeiten gilt: Je größer der Input an Daten, desto besser die Ergebnisse. 5G-Netzwerke generieren die enormen Datenmengen, die KI für ihren Betrieb benötigt. Gleichzeitig kann KI dabei helfen, die Komplexität zu managen und die 5G-Netze zu schützen.

Laut einem Bericht von Ericsson „What role will Artificial Intelligence have in the mobile networks of the future?"[73], wird KI zunehmend von CSPs in mobile Netzwerke übernommen. Anwendungen von KI, die bereits von CSPs implementiert wurden, sind u. a. die intelligente **Erkennung und Vorhersage von Anomalien**, die Planung von Netzkapazitäten und die intelligente Filterung der Netzalarme.

Um das Potenzial, aber auch die Herausforderungen von KI weiter zu verdeutlichen, ist es das Ziel von CSPs und Entscheidungsträgern im Allgemeinen, ein sogenanntes **„Zero-Touch"-Netzwerk** aufzubauen. Diese Netzwerke werden sich dadurch auszeichnen, dass außer High-Level-Deklarationen und -Implementierungen keine menschlichen Eingriffe mehr erforderlich sind.[74] Das System misst und versteht den Kontext und reguliert das Netzwerk. Obwohl dies außerordentlich vorteilhaft und kosteneffizient ist, bedeutet es auch einen Verlust an Kontrollierbarkeit und die Notwendigkeit neuartiger Methoden und Indikatoren zur Messung der tatsächlichen Zuverlässigkeit (Sicherheit) und Leistung des gesamten KI-Systems.

Risikoanalyse und Kostenbewertung

Die Grundlage für den Einsatz von KI ist der Trainingsprozess, der für die Bereitstellung genauer und zuverlässiger Ergebnisse entscheidend ist. Das Training (und die Verfeinerung) ist ein fortlaufender Prozess, der die riesige Menge an Daten nutzt, die von den 5G-Netzwerkgeräten erzeugt werden. Die Qualität der Trainingsdaten ist daher entscheidend für die Steuerungsaktionen der KI. Wenn ein Fehler oder eine Verzerrung in den Eingabedaten vorliegt, wirkt sich dies auf den Betrieb und die Geschäftsdienste des CSP aus. Im Falle einer absichtlichen Manipulation können die Trainingsdaten absichtlich verändert werden, um eine KI zu falschen Aktionen zu zwingen, was schwerwiegende Folgen in Bezug auf Kosten, Effizienz und Sicherheit hätte.

Es ist nicht einfach, die versteckten Kosten zu identifizieren und zu quantifizieren, die mit der Einführung von KI in 5G verbunden sind, wenn Geräte von nicht-vertrauenswürdigen Anbietern eingesetzt werden. Ein möglicher Ansatz ist die Interaktion und das Sammeln von Informationen in qualitativer und quantitativer Hinsicht direkt von CSPs. Tatsächlich gibt es in der akademischen Literatur keine allgemeingültigen Kostenmodelle oder Analysen, die für Evaluierungszwecke genutzt werden könnten. KI ist eine aufstrebende Technologie, und der Schwerpunkt der aktuellen F&E-Arbeiten liegt hauptsächlich auf der Erforschung ihrer Vorteile, wobei eine vollständig kontrollierte und sichere 5G-Netzwerkumgebung vorausgesetzt wird.

Es muss eine mehrdimensionale Bewertung herbeigeführt werden, denn relevant sind sowohl

1. ökonomische (z. B. Einnahmeverluste bei verminderten Abonnements),

73 Ericsson (2019).
74 Ekudden (2018), S. 3.

2. soziale (z. B. Innovationshürden),

3. technische (z. B. Effizienzverlust, geringe Servicequalität) als auch

4. politische (z. B. Vertrauensverlust, Schwierigkeiten bei der Einhaltung von Vorschriften)

Aspekte. Da sich mehrere Kostendimensionen mit der KI-Technologie (und ihren Anwendungen) befassen, wird im folgenden Abschnitt versucht, die Art der Kosten zu klären.

Die Entwicklungspläne der befragten Mobilfunknetzbetreiber sehen eine vollständige Einführung von KI-basierten Netzwerk-Controllern in der zweiten Phase der 5G-Implementierung vor. Infolgedessen werden die meisten von ihnen die sich daraus ableitende Bedrohung für das Netzwerk erst in dieser Phase in Betracht ziehen. Da KI jedoch auf den Daten basieren wird, die von den heute installierten Netzwerkgeräten gesammelt werden, haben die Planungen für den zukünftigen Netzausbau einen Einfluss auf die heutige Entscheidung bezüglich der Auswahl des Zulieferers der Netzwerktechnologie.

Es gibt drei Arten von Kosten bei Fehlfunktionen eines KI-Systems aufgrund einer Daten- oder Modellschädigung:

1. Kosten der Problemerkennung

2. Kosten für den entstandenen Schaden

3. Kosten für die Behebung des Problems (z. B. Rip-and-Replace)

Kosten der Problemerkennung

Für diese Kosten ist es entscheidend, dass in regelmäßigen Abständen eine Wirkungsanalyse durchgeführt wird, um zu überprüfen, ob das KI-System ordnungsgemäß funktioniert. Zu diesem Zweck müssen Aktivitäten der Datensammlung, -analyse und -validierung (für Datenströme oder -pools) durchgeführt werden. Kosten dieser Art sinken mit dem Anstieg an Vertrauen und Zuverlässigkeit in die KI-Leistung und deren Lieferanten.

Kosten für den entstandenen Schaden

Diese Kosten entstehen im wirtschaftlichen, sozialen, technischen und im politischen Bereich. Beispiele können sein: (i) Verlust von Marktanteilen (z. B. durch Kundenabwanderung aufgrund niedriger Servicequalität), (ii) Verlust von Glaubwürdigkeit (z. B. durch unzuverlässige Services oder Service-Support-Systeme), (iii) Verlust von Wettbewerbsvorteilen (z. B. durch unzureichende Angebote oder geringere Effizienz), (iv) schlechte Netzplanung oder Betrieb & Wartung, (v) Strafe oder Bußgeld für die Nichterfüllung von Service-Level-Agreements oder die Einhaltung von Vorschriften.

Kosten für die Problembehebung

Die Behebung von Anomalien ist ein komplexer Vorgang, insbesondere bei potenziell allgegenwärtigen KIs. Diese Kosten sind identisch mit der Minderung oder dauerhaften Behebung eines Sicherheitsrisikos. Allerdings ist in diesem Fall ein Rip-and-Replace ohne einen längeren Ausfall zumindest von Teilen des Mobilfunknetzes unwahrscheinlich: Das (Neu-) Training des KI-Systems kostet Zeit und Ressourcen und gehören daher zu denen mit den größten Auswirkungen.

Die kontaktierten Mobilfunknetzbetreiber sind sich einig, dass KI-Systeme, die für Kerndienste (z. B. Anomalieerkennung und automatische Generierung von Trouble Tickets) eingesetzt werden, sicher genug sind, um in einer geschützten Umgebung zu arbeiten. Sie haben jedoch Bedenken, wenn KI für das Management und die Orchestrierung des Netzwerks eingesetzt wird. Eine Überlegung stammt aus einem aktuellen Nokia-Bericht[75], der eine 5G-Implementierungsarchitektur vorschlägt, die Bedrohungsbehebungen auf der Anwendungsebene hinzufügt. Die vorgeschlagene Architektur geht laut der EU 5G-Toolbox von einer zugrundeliegenden heterogenen technologischen Ebene aus (d. h. verschiedene technologische Anbieter).

75 Nokia (2020).

6.2.5 Regulierungskosten

Die potenzielle Beteiligung von nicht-vertrauenswürdigen Anbietern in der 5G-Infrastruktur erfordert zusätzliche Anstrengungen und Aufwendungen für Sicherheitsvorschriften im Rahmen der Netzausrüstung im **politischen und legislativen Prozess** sowie für Netzbetreiber, die diese Ausrüstung verwenden. Netzbetreiber tragen das Risiko einer fahrlässigen Verletzung bestimmter Vorschriften. Die Akteure, die für die Formulierung der Gesetzgebung verantwortlich sind, müssen zusätzliche Parameter definieren, die eine sichere Netzwerkumgebung gewährleisten und gleichzeitig faire Wettbewerbsbedingungen garantieren. Selbst wenn ein nicht-vertrauenswürdiger Anbieter die notwendige Ausrüstung für die 5G-Infrastruktur bereitstellt, müssen der gesetzliche Rahmen und die Regulierung beispielsweise die Datensicherheit der Nutzer gewährleisten, entweder innerhalb des ausgerüsteten Netzes oder mit zusätzlichen Regelungen für Systeme, die mit dem Netz verbunden sind.

Bevor eine Verordnung oder ein Gesetz verabschiedet wird, sind viele Instanzen am Beratungs-, Gesetzgebungs- und Umsetzungsprozess beteiligt. Stakeholder und Entscheidungsträger sind die Ministerien und parlamentarische Gremien, die neben den zuständigen Behörden, Industrieverbänden, Standardisierungs- und Prüfungsinstitutionen sowie Netzbetreibern für das Querschnittsthema zuständig sind. Im Gegensatz zu einem Markt, in dem die technische Infrastruktur nur von vertrauenswürdigen Anbietern bereitgestellt wird, müssen mögliche Bedrohungen durch nicht-vertrauenswürdige Anbieter rechtlich untersucht und Maßnahmen zur Vermeidung möglicher Sicherheitslücken im Rahmen des Gesetzgebungsverfahrens ausgewertet werden.

Für politische Institutionen und Behörden bedeutet dies einen erhöhten Aufwand durch komplexere Entscheidungsprozesse (z.B. ressortübergreifende Abstimmungen) und einen höheren personellen Aufwand aufgrund der Quantität und Qualität regulativer Vorgaben und des Zukaufs externer technischer und juristischer Expertise vor Verabschiedung eines entsprechenden Gesetzes. Die Kosten der Regulierung (bzw. das Risiko von Sanktionen und Bußgeldern bei Nichteinhaltung) sind also eine Belastung nicht ausschließlich für die Akteure, die sie einhalten müssen. Nach und nach entstehen auch dem Geldgeber des Regulierers (meist dem Steuerzahler) Kosten, die durch den Regulierungsprozess selbst anfallen. Dies gilt sowohl für das ausgerüstete Netz als auch für alle Regulierungen von angeschlossenen Systemen.

Einmal verabschiedet, bedeutet eine komplexere Regulierung, die insbesondere dann notwendig ist, wenn ein vertrauensunwürdiger Anbieter Teil der 5G-Infrastruktur ist, mehr **Kosten für jeden Marktteilnehmer**, der unter dieser Regulierung arbeitet, sowie für die Prüfbehörden. Das Vorhandensein eines nicht-vertrauenswürdigen Anbieters erhöht die Nachfrage nach der Bereitstellung von technischem Fachwissen in einer Prüfbehörde und führt aufgrund der komplexeren Regulierung sowie der Häufigkeit und Intensität der Prüfungen zu höheren Verwaltungskosten. Um diesem Bedarf gerecht zu werden, steigen die Kosten der Prüfbehörden entweder durch die Beschäftigung von mehr und gut ausgebildetem und knappem Personal oder durch die Beauftragung von zertifizierten externen Diensten, die in der Lage und verfügbar sind, die Prüfung durchzuführen. So hat z.B. das Bundesamt für Sicherheit in der Informationstechnik acht Anbieter nach Common Criteria for Information Technology Security Evaluation, CC zertifiziert.[76] Neben der Zertifizierung kann der Bedarf an häufigeren Audits nur gedeckt werden, wenn die Dienstleister über genügend Kapazitäten verfügen, um diese Aufgabe zu übernehmen. Ein Mangel an geschultem oder verfügbarem Personal beim Anbieter führt zu Verzögerungen der Auditierungsprozesse und zu höheren Kosten für die Behörden.

Marktteilnehmer wie Netzbetreiber sind verpflichtet, die Vorschriften einzuhalten. Um die komplexeren Vorschriften zu erfüllen, kommen auf die Unternehmen vermutlich zusätzliche Kosten durch Schulungen und Kommunikation, die Entwicklung ebenso komplexer und strenger Zertifizierungen für ihre Lieferanten und das Risiko von Klagen nach Verstößen zu. Zusätzlich müssen diese spezifischeren und umfangreicheren Regelungen umfassend auf das Unternehmen übertragen werden. Dies kann thematisch erweiterte Verbindungsbüros, Unterstützung durch Rechtsberater, Workshops z. B. für das Einkaufspersonal und einen kontinuierlichen Austausch mit den zuständigen Behörden und Entscheidungsträgern erfordern.[77]

76 BSI (2020).
77 Voland und Büsch (2020).

Foto © gremlin/iStockphoto

Regulierungskosten können nur dann als Teil der versteckten Kosten von nicht-vertrauenswürdigen Anbietern definiert und berechnet werden, wenn Gesetze, sowie der zusätzliche Aufwand und die zusätzlichen Kosten ausschließlich als Folge oder Gegenmaßnahme im Hinblick auf vertrauensunwürdige Anbieter bestimmt werden. Während das generelle Vorhandensein von nicht-vertrauenswürdigen Anbietern detailliertere Regelungen und damit einen erhöhten Aufwand für deren Umsetzung und Einhaltung erfordert, kann nicht quantifiziert werden, welcher Teil der zusätzlichen Kosten ausschließlich durch diese Anbieter entsteht.

Zertifizierungen für z.B. bestimmte IT-Sicherheitsstufen von Geräten werden ohnehin gelten, um potenzielle Angreifer abzuwehren, unabhängig von der Vertrauenswürdigkeit der Hersteller. Dennoch gibt die Darstellung des Ergebnisses ausgewählter Regulierungen einen Eindruck vom budgetären Umfang der Regulierungskosten im Bereich der IT-Sicherheit. Nachfolgend finden Sie in Tabelle 6 Abschätzungen zu themenbezogenen Regulierungen für Deutschland, die vom Nationalen Normenkontrollrat zur Verfügung gestellt wurden.

Tabelle 6: Erwartete jährliche Kosten für die Einhaltung ausgewählter Vorschriften (deutsche Beispiele)

Cost bearer	*Required Expenses (extracts)*	*Expected amount in €*
	IT Security Act 2015[78]	
Administration	Staff (425 additional posts) at BSI (220), BKA (80), BfV (50), other authorities (75), material costs	38,000,000
Economy	Reporting security incidents	9,000,000
		47,000,000
		+ 6,000,000 (non-recurring)
	Implementation of EU Directive 2016/1148 in Germany (NIS Directive)[79]	
Administration	Staff (181,5 additional post), mainly at the BSI	14,300,000
Economy	Reporting security incidents	13,200,000
		27,500,000
	IT Security Act 2.0 (expected 2021)[80]	
Administration	Staff (948 additional posts) at BSI (799), BKA (90), BNetzA (34), BDBOS (21), BMI (4), material costs	125,800,000
Economy	Reporting security incidents	9,000,000
		134,800,000
		+ 28,800,000 (non-recurring)

Quelle: Normenkontrollrat, eigene Darstellung.

Darüber hinaus beinhaltet der Einsatz von nicht-vertrauenswürdigen Anbietern das Potenzial einer ungewollten Verletzung von Vorschriften durch den Netzbetreiber, der beispielsweise für ein Datenleck oder eine allgemeine Sicherheitsverletzung zur Verantwortung gezogen werden könnte. Als Vorsichtsmaßnahme müssen Unternehmen ihre Auditierung und Zertifizierung von Lieferanten verstärken, was eine erweiterte Testinfrastruktur, geschultes Personal, Beschaffungsspezifikationen und weitere technische und prozessuale Investitionen erfordert. Dieser zusätzliche Aufwand soll gewährleisten, dass der Netzbetreiber bei Vorwürfen von Anwendern oder der Prüfbehörde selbst Klagen oder Schadensersatzforderungen wegen Verletzung von Datenschutzvorschriften entgeht. Beispielsweise führen Verstöße gegen das IT-Sicherheitsgesetz in Deutschland zu Bußgeldern in Höhe von zwei % des weltweiten Jahresumsatzes bis zu 10 Mio. Euro; in besonderen Fällen vier % des Jahresumsatzes bis zu 20 Mio. Euro. Ungeachtet der Herkunft des Gerätelieferanten ist das Unternehmen, das gegen die Vorschrift verstößt, die haftende Einheit.

Darüber hinaus kann die Nichteinhaltung der Vorschriften zu einer Unterbrechung des Datenflusses führen und – je nach Vertragskündigung – die Rentabilität des Netzwerks schwächen. Letztendlich könnte man in einem Rip-and-Replace-Szenario landen, in dem die nicht-vertrauenswürdige Technologie durch die von vertrauenswürdigen Anbietern ersetzt werden muss, trotz aller vorherigen Bemühungen, dies zu vermeiden.

6.2.6 Versicherung gegen Cyberrisiken

Die Cyberversicherung ist ein **Instrument des Risikomanagements**. Ein Unternehmen überträgt das Cyberrisiko gegen einen Preis auf den Versicherer. Der Preis ist abhängig von der Größe des Risikos und sinkt, wenn das Unternehmen mehr für seinen Cyberschutz tut.

In Deutschland haben bereits 14 % der Unternehmen eine Cyberversicherung abgeschlossen, einschließlich 32 % aller größeren Firmen.[81] In Frankreich, wo die Gesamtsumme der Versicherungsprämien im Jahr

78 Normenkontrollrat (2014).
79 Normenkontrollrat (2016).
80 BMI (2020).
81 Bitkom (2018), S. 51.

2018 80 Mio. Euro betrug, wächst der Markt schnell, ist aber im Vergleich zu den USA immer noch sehr klein. Hinter diesem Betrag verbergen sich große Unterschiede: Nach kostspieligen Angriffen auf Saint Gobain oder Renault schließen inzwischen nahezu alle der großen und börsennotierten Unternehmen in Frankreich eine Cyberversicherung ab. Am anderen Ende des Spektrums schließen nur ein paar % der KMU und sehr kleinen Unternehmen (die mehr als 99 % der französischen Unternehmen ausmachen) eine solche Cyberversicherung ab.[82]

Schäden, die durch Angriffe auf 5G-Netze entstehen, müssen von jemandem getragen werden, entweder vom Netzbetreiber oder von dessen Kunden. Wenn der Mobilfunknetzbetreiber für den Schaden haftet, ist ein gängiger Weg, mit diesem Risiko umzugehen, eine Versicherung abzuschließen. Die Versicherung wird jedoch typischerweise verlangen, dass der Netzbetreiber bestimmte Sicherheitsstandards erfüllt, damit die Versicherung den Schaden abdeckt. Der Versicherer könnte somit zu einer Quasi-Regulierungsbehörde für den 5G-Ausrüstungsmarkt werden. Da diese Arten von neuen Risiken aufgrund fehlender Daten aus der Vergangenheit schwer zu kalkulieren sind, werden die Versicherer ihre Risikoexposition auf genau definierte Schäden beschränken und die Deckung begrenzen. Diese Grenzen sind schnell erreicht, wenn Betriebsunterbrechungen durch die Police abgedeckt sind.

Von 2017 bis 2019 führte IRT SystemX eine Studie durch, um das Management von Cyberrisiken entlang der gesamten Wertschöpfungskette und deren Übertragbarkeit auf Versicherungen zu untersuchen.[83] [84] Die Studie hob *"the lack of prior experience about previous cyber incidents"* hervor, mit dem Versicherungsunternehmen konfrontiert sind. Die Studie beleuchtete auch den erschwerenden Faktor des stillen Schutzes, oder nicht-affirmativen Schutzes. Im Vergleich zu anderen Risikokategorien verfügen Versicherungsunternehmen über weniger als 10 Jahre an Aufzeichnungen über Cybervorfälle. Diese kurze Historie deckt nicht alle Arten von Vorfällen ab und noch weniger haben bisher zu Schäden geführt. Die vorhandene Historie bezieht sich hauptsächlich auf Ransomware-, Malware- und Phishing-Vorfälle, obwohl es noch viele andere Kategorien gibt. Außerdem birgt jede neue Technologie - und 5G ist hierfür das perfekte Beispiel - neue Arten von Risiken.

In 5G-Netzen ist die **Bewertung der Entschädigungskapazität von Versicherungen jedoch komplexer** und problematischer, insbesondere bei Vorhandensein von nicht-vertrauenswürdigen Anbietern. Versicherungsunternehmen, die das Risiko von Rechtsverletzungen in solchen Kontexten abdecken, werden für ihre Angebote in Kommunikationsumgebungen mit nicht-vertrauenswürdigen Anbietern wahrscheinlich höhere oder sogar **prohibitiv hohe Prämien** verlangen oder das Risiko aus Sicht des Versicherers **als nicht abdeckbar einschätzen**. Für die Gesellschaft könnte dies bedeuten, dass der Staat als Versicherer der letzten Instanz einspringen muss, wie es bei der Atomenergie der Fall war. Mehrere europäische Regierungen mussten Bürgschaften für Kernkraftwerke privater Energieversorger übernehmen, da das neue „nukleare" Risiko von den Versicherern als nicht versicherbar eingestuft wurde. Eine ähnlich komplexe Situation könnte entstehen, wenn sich Versicherer auf eine Kriegsrisikoklausel berufen, wenn eine ausländische Regierung hinter einem Angriff vermutet wird.

Derzeit verfügen die Versicherer nicht über alle versicherungsmathematischen Elemente, die sie benötigen, um ihr Versicherungsangebot für 5G-Netzwerke zu dimensionieren, insbesondere im Hinblick auf immaterielle Daten, die noch nicht rechtlich qualifiziert oder finanziell und buchhalterisch quantifiziert sind. Ohne eine zuverlässige Risikoanalysemethode und eine umfassende Historie von Cybervorfällen bleiben die Grenzen dieses Risikos unklar und die Folgen auf globaler Ebene scheinen unkontrollierbar. In einem solchen Kontext werden Versicherer und Rückversicherer ihre Policen wahrscheinlich anpassen, wenn ihre Kunden beginnen, ihre Produktion an 5G-Netzwerke anzuschließen. Strenge Haftungsgrenzen in den Versicherungspolicen scheinen wahrscheinlich. Es wird also interessant sein zu sehen, ob Versicherer bei der Wahl des Telekommunikationsbetreibers eine vorschreibende Rolle spielen werden, insbesondere für sicherheitssensible Akteure und Unternehmen mit einem höheren Bedrohungsgrad in Bezug auf geistiges Eigentum und Datenschutz.

82 Commission ad hoc Cyber Risk (2018).
83 Cotelle et al. (2015).
84 Cotelle et al. (2019).

6.3 Verschiebung der Nachfrage

Eine Einbeziehung von nicht-vertrauenswürdigen Anbietern in europäische 5G-Netze könnte zum vorvertraglichen Verlust von **sicherheitssensiblen Kunden** und möglicherweise sogar zu deren Abwanderung führen. Diese Kunden würden sicherstellen, dass sie sich von Anbietern fernhalten, die ihrerseits oder mit ihren Kunden über unsichere 5G-Netze kommunizieren oder Daten und Informationen verarbeiten. Dies betrifft insbesondere **staatliche Auftraggeber** wie Militär, Nachrichtendienste und Sicherheitsbehörden, aber auch Bundes- und Landesministerien und nachgelagerte Institutionen. Bestimmte Teile der Privatwirtschaft, wie **Anbieter kritischer Infrastrukturen**, sollten die gleichen Vorsichtsmaßnahmen ergreifen. Man denke nur an den Stromnetzbetreiber 50Hertz, an dem ein chinesisches Unternehmen 20 % der Anteile kaufen wollte. Dieser Deal wurde letztlich von der deutschen Regierung aus Sicherheitsgründen verhindert; sie befürchtete, dass China die Kontrolle über lebenswichtige deutsche Versorgungsunternehmen übernehmen könnte. [85]

Es gibt verschiedene Definitionen dessen, was kritische Infrastrukturen sind, und die Zusammensetzung der Sektoren unterscheidet sich sogar zwischen den EU-Mitgliedsländern. Üblicherweise werden die folgenden Sektoren genannt:

- Energie,
- Informationstechnologie,
- Telekommunikation,
- Verkehr,
- Gesundheit,
- Wasser,
- Ernährung,
- Finanzen und Versicherung.

Diese Sektoren werden in der Volkswirtschaftlichen Gesamtrechnung nicht eins zu eins abgebildet. Dennoch ist es möglich, zumindest für einige von ihnen Näherungswerte abzuleiten, indem man öffentliche Dienste, Gesundheit, Bildung (18,8 %), Finanz- und Versicherungsdienstleister (3,9 %), Information und Kommunikation (4,6 %) zusammenzählt, also insgesamt 27,3 %.[86] Unter der Annahme, dass sich dieser Anteil in der Struktur der Geschäftskunden des Telekommunikationssektors widerspiegelt – ein Viertel davon gehört zu den kritischen Infrastrukturen – leiten wir ab, dass sich bis zu 27 % des Umsatzes des Kommunikationssektors (öffentlicher Sektor und Geschäftskunden) zu Mobilfunknetzbetreiber mit ausschließlich vertrauenswürdigen Anbietern verlagern könnten. Entweder wechseln diese Kunden aus kritischen Infrastrukturen zu Anbietern, die mit vertrauenswürdigen Netzausrüstern zusammenarbeiten, bauen eigene Campusnetze auf oder entscheiden sich zumindest bei sicherheitssensiblen Anwendungen gegen den Einsatz der 5G-Technologie.

Während die erste Verschiebung – Kunden wechseln den Betreiber – für die Betreiber eher eine betriebswirtschaftliche Überlegung bei der Entscheidung über die Wahl des Anbieters ist, fällt sie dennoch in die Kategorie der versteckten Kosten. Der Verzicht auf den Anschluss an 5G-Netze und die damit verbundenen entgangenen Produktivitätsgewinne stellen externe Kosten der Entscheidung des Mobilfunknetzbetreibers dar, von wem er die Netztechnologie beziehen möchte.

Die Größe der möglichen Nachfrageverschiebung von Anbietern kritischer Infrastrukturen (siehe Tabelle 7 unten) könnte wie folgt berechnet werden:

85 BMWi (2018).

86 Statistisches Bundesamt (2020). Die Definition von kritischen Infrastrukturen in Deutschland (Organisationen oder Einrichtungen von erheblicher Bedeutung für das staatliche Gemeinwesen, deren Ausfall oder Beeinträchtigung zu nachhaltigen Versorgungsengpässen, erheblichen Beeinträchtigungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde) orientiert sich an Wirtschaftssektoren. Bitte beachten Sie, dass der Sektor Bildung vom Statistischen Bundesamt in einer Kategorie mit dem Öffentlichen Dienst und dem Gesundheitswesen geführt wird und hier rechnerisch nicht herausgerechnet werden kann.

$$D_t^{mtl\ cr} = R_t^{tl} * S_t^{mts} * Sh_t^{bc} * GDP_t^{cr}$$

mit

$D_t^{mtl\ cr}$ = Nachfrage der kritischen Infrastrukturindustrien nach mobilen Telekommunikationsdiensten

R_t^{tl} = Umsatz mit Telekommunikationsdiensten im Zeitraum Jahr t

S_t^{mts} = Anteil der mobilen Telekommunikationsdienste an den Gesamtdiensten im Zeitraum Jahr t

Sh_t^{bc} = Anteil der Geschäftskunden an allen Kunden im Zeitabschnitt Jahr t

GDP_t^{cr} = relativer Beitrag der kritischen Infrastrukturindustrien zum BIP im Zeitabschnitt Jahr t

t = Zeitraum, Jahr der Betrachtung

Tabelle 7: Mögliche Verschiebung der Nachfrage kritischer Infrastrukturindustrien weg von MNOs, die nicht-vertrauenswürdige Netzwerke betreiben

Kritische Infrastrukturindustrien	Verschiebung der Nachfrage
Deutschland	2.496.501.000 €
Frankreich[87]	474.880.000 €
Italien	929.235.000 €
Portugal[88]	97.238.000 €

Quelle: eigene Schätzungen.

Eine weitere Verschiebung – oder das Ausbleiben einer Verschiebung – betrifft die Standortwahl von sicherheitssensiblen Unternehmen aus dem Ausland. Diese werden ihren Standort nicht zuletzt von der Existenz eines sicheren Kommunikationsnetzes in den Ländern abhängig machen, die für ihre ausländischen Direktinvestitionen (foreign direct investment – FDI) in Frage kommen.[89]

Weitere sicherheitssensible Kunden sind der Sicherheits- und Verteidigungssektor, F&E-intensive Industrien oder andere Branchen mit besonderen Sicherheitsrisiken. F&E-intensive Aktivitäten sind besonders anfällig für Unternehmens- oder Staatsspionage und die Verletzung von geistigem Eigentum (intellectual property rights, IPR). Zu den relevanten Sektoren gehören Pharmazie, Elektronik, Nanotechnologie und mehr. Man denke nur an die vielen aktuellen Spionageversuche rund um die Coronavirus-Impfstoffentwicklung.[90]

87 Die Zahl für Frankreich scheint im Vergleich zu der für Deutschland überraschend niedrig zu sein, aber einerseits war der Umsatz der Telekommunikationsdienstleister in Frankreich insgesamt nur gut halb so groß, zum anderen ist der Anteil der Geschäftskunden in Deutschland knapp doppelt so groß. Weiterhin ist der Beitrag der KRITIS-Unternehmen zum Bruttoinlandprodukt in Frankreich prozentual geringer als in Deutschland.

88 Die niedrige Zahl ist auf eine sehr enge Definition dessen zurückzuführen, was in Portugal als kritische Infrastruktur gilt.

89 Sicherheit in verschiedenen Dimensionen wurde als statistisch hochsignifikante Bedingung für FDI ermittelt, z.B. von Busse und Hefeker (2007) in Bezug auf „Regierungsstabilität, interne und externe Konflikte, Korruption, ethnische Spannungen, Recht und Ordnung, demokratische Rechenschaftspflicht der Regierung und Qualität der Bürokratie" ("government stability, internal and external conflict, corruption, ethnic tensions, law and order, democratic accountability of government, and quality of bureaucracy") (Hammami et al., 2020).

90 Williams (2020).

Der globale Handel mit digitalen Gütern und Dienstleistungen gewinnt sowohl im Inland als auch im internationalen Handel immer mehr an Bedeutung. Die Nutzung von Big Data birgt ein erhebliches Potenzial an Umsatzwachstum von 2,9 % und bis zu 3,6 % Kostenreduktion pro Jahr.[91] Das jährliche Bruttoinlandsprodukt in Europa könnte bis 2025 um bis zu 1,9 Billionen Euro steigen, wenn Datenanalysen und das Internet der Dinge implementiert und genutzt werden[92]. An diesem Trend zu mehr digitalem Handel aus Risikoscheu nicht teilzunehmen, bedeutet hohe Opportunitätskosten und ein Zurückfallen hinter den Wettbewerb.

Alle Branchen, die für ihre Geschäftstätigkeit auf die Verfügbarkeit und Integrität ihrer Datenströme angewiesen sind, wollen diese absichern. Branchen mit ausgeprägten Sicherheitsanforderungen müssen vor Manipulationen und daraus resultierenden Risiken für Menschenleben und körperliche Unversehrtheit geschützt werden, darunter die Raumfahrt, die Luftfahrt, die Automobilindustrie, die Robotik und andere. Die Anbindung an ein 5G-Netz mit nichtvertrauenswürdigen Komponenten werden sie sich zweimal überlegen.

Ein möglicher Ansatz zur Quantifizierung der Auswirkungen eines solchen Vorvertragsverlustes ist die Analyse von Daten zu den staatlichen Ausgaben für Telekommunikationsdienste. Diese Daten sollten in den Regierungsbudgets verfügbar sein. Man könnte dies mit der Anzahl der vergleichbaren sicherheitssensiblen Regierungsstellen multiplizieren und so die potenziellen Gesamtumsatzeinbußen für Mobilfunknetzbetreiber abschätzen. In einem weiteren Top-Down-Ansatz kann man davon ausgehen, dass die IPR-intensive Industrie der sicherheitssensiblen Industrie entspricht. Etwa 45 % der gesamten wirtschaftlichen Aktivität (BIP) in der EU ist auf IPR-intensive Industrien zurückzuführen, was einem Wert von 6,6 Billionen Euro entspricht.[93] Wenn man weiter davon ausgeht, dass sich die Kosten für Telekommunikationsdienste genauso verteilen wie ihr Anteil am BIP, könnten 45 % des Umsatzes mit Geschäftskunden zu einem Betreiber mit ausschließlich vertrauenswürdigen Anbietern verlagert werden oder 5G komplett vermeiden.

Der Umfang der möglichen Verlagerung von IPR-intensiven Kunden (siehe Tabelle 8 unten) könnte wie folgt berechnet werden:

$$D_t^{mtl\ ipr} = R_t^{tl} * S_t^{mts} * Sh_t^{bc} * GDP_t^{ipr}$$

mit

$D_t^{mtl\ ipr}$ = Nachfrage von IPR-intensiven Industrien nach mobilen Telekommunikationsdiensten

R_t^{tl} = Umsatz von Telekommunikationsdiensten im Zeitraum Jahr t

S_t^{mts} = Anteil der mobilen Telekommunikationsdienste an den Gesamtdiensten im Zeitraum Jahr t

Sh_t^{bc} = Anteil der Geschäftskunden an allen Kunden im Zeitabschnitt Jahr t

GDP_t^{ipr} = relativer Beitrag der IPR-intensiven Branchen zum BIP im Zeitraum Jahr t

t = Zeitraum, Jahr der Betrachtung

91 Brookings Institution (2017).
92 Bughin et al. (2016).
93 EUIPO (2019).

Tabelle 8: Potenzielle Verschiebung der Nachfrage von Industrien, die geistige Eigentumsrechte benötigen, weg von Mobilfunknetzbetreibern, die nicht-vertrauenswürdige Netzwerke betreiben

IPR-intensive Industrien	Verschiebung der Nachfrage
Deutschland[94]	4.613.904.000 €
Frankreich	1.018.618.000 €
Italien	1.259.570.000 €
Portugal	344.386.000 €

Quelle: eigene Schätzungen.

Es ist uns bewusst, dass es eine Überschneidung zwischen der IPR-intensiven und der kritischen Infrastrukturindustrie gibt. Allerdings können einige Teile von KRITIS nicht unbedingt als IPR-intensiv angesehen werden (wie Wasserversorgung, Landwirtschaft usw.) und umgekehrt. Es ist daher sicher, dass hier mehr als die Hälfte und bis zu zwei Drittel aller Geschäfte von Netzbetreibern mit Firmenkunden in Frage kommen und tendenziell in Richtung vertrauenswürdige Netze wandern sollten.

Für KRITIS ist auch absehbar, dass die Verwendung von ausschließlich vertrauenswürdigen Netzwerken in Zukunft durch Regulierung vorgeschrieben werden könnte, und für andere Unternehmen könnten Cyberversicherungen dies zur Bedingung für ihre Kunden oder ihre Anbieter machen, die Teil einer Wertschöpfungskette sein wollen (z. B. in der Automobilindustrie). Da die Vorteile von 5G hauptsächlich in Geschäftsanwendungen liegen, prognostizieren wir daher, dass das Geschäftsvolumen der Mobilfunknetzbetreiber mit Firmenkunden relativ zunehmen sollte.

Diese potenzielle Verschiebung der Nachfrage von Unternehmenskunden sollte im Zusammenhang mit den aktuellen Kostenforderungen von Mobilfunknetzbetreibern bezüglich Rip-and-Replace gesehen werden. Die ausschließliche Verwendung von vertrauenswürdigen Anbietern für 5G-Netze könnte dazu beitragen, den Umsatz mit Firmenkunden zu halten und sogar zu steigern.

Redundante Infrastruktur

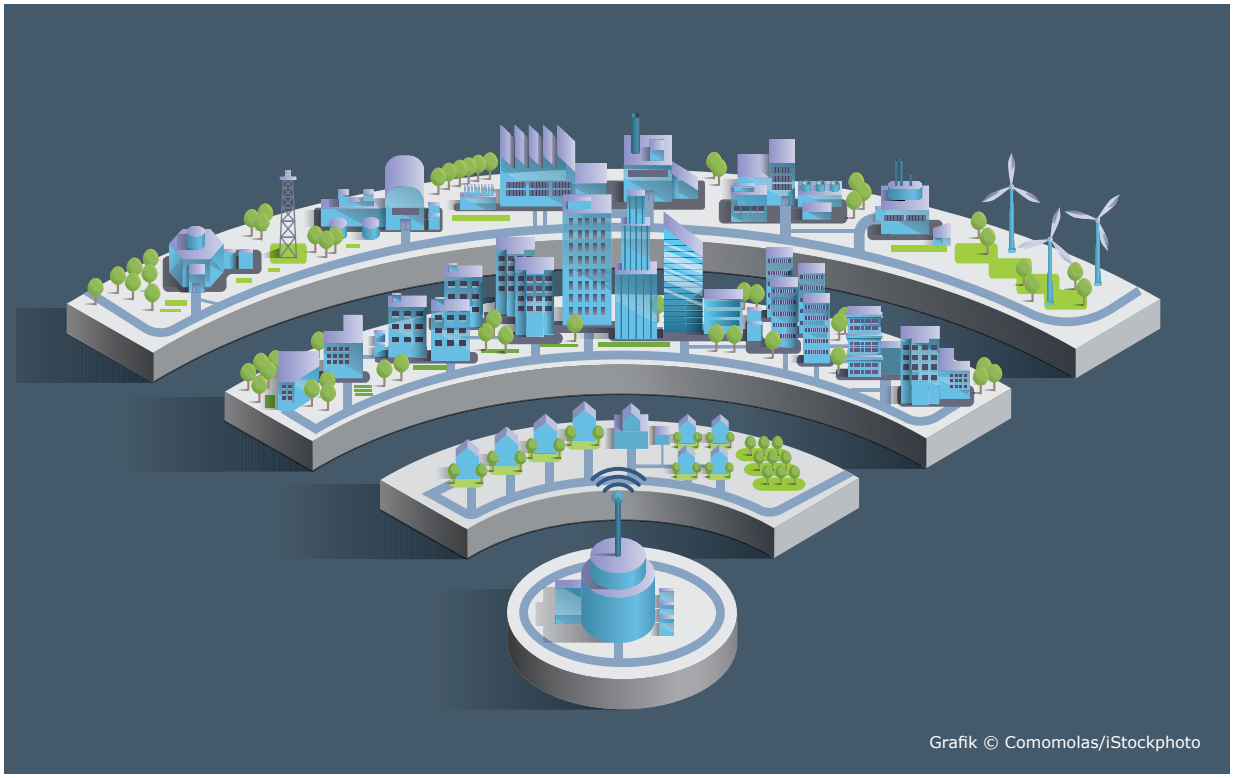
Da wir die ökonomischen Auswirkungen für die gesamte Gesellschaft und nicht die betriebswirtschaftlichen Konsequenzen für einzelne oder alle Unternehmen der Telekommunikationsbranche betrachten, läuft die interessante Frage darauf hinaus: Wie viel teurer würde es für die Gesellschaft werden, wenn die Regierung eine Make-or-Buy-Entscheidung zugunsten eines staatlichen Netzes treffen würde? Ausgehend von der Annahme, dass ein staatlicher Kommunikationsanbieter, der in einigen Ländern erst gegründet werden muss, weniger effizient ist als ein privater, wäre die wirtschaftliche Belastung einer solchen ineffizienten Second-Best-Lösung die Differenz der Vollkostenpreise zwischen dem staatlichen und dem privaten Netz.

Als Beispiel dafür, wie kostspielig der sicherheitsmotivierte Aufbau einer redundanten staatlichen Kommunikationsinfrastruktur ist, steht das Netz des Bundes in Deutschland. In der Planungsphase wurde davon ausgegangen, dass (neben den anfänglichen Kosten für die Überführung in den Regelbetrieb von 100 Mio. Euro durch Bundesinstitutionen) die jährlichen Erfüllungskosten von ca. 92,2 Mio. Euro aus dem Betrieb des Bundesnetzes weit unter den Kosten von ca. 160 Mio. Euro pro Jahr liegen würden, die bei einem externen Betrieb des Bundesnetzes entstehen würden.[95] Das Projekt geriet später aus dem Ruder, was die Finanzierung und die Verzögerungen

94 Der Grund dafür, dass die Kosten in Deutschland im Vergleich zu Italien und Frankreich so viel höher sind, ist die höhere IPR-Intensität der Wirtschaft und ein viel größerer Anteil an Geschäftskunden auf dem Markt für mobile Dienste.

95 Bundesrat (2016).

angeht. Weil sich das Projekt Netz des Bundes um sechs Jahre verzögerte und die Kosten von 114 auf 426 Mio. Euro gestiegen waren[96], hat das Finanzministerium die Ausgaben für das Projekt im Jahr 2020 gesperrt.[97] Mit anderen Worten: Der Aufbau der Infrastruktur war mit zusätzlichen versunkenen Kosten in Höhe von 312 Mio. Euro verbunden. Der größte Teil davon entfiel auf angemietete, aber ungenutzte Rechenzentren, die Beschaffung teurer Hardware, die nicht genutzt wurde, und Kosten für schlecht betreute externe IT-Berater.



Grafik © Comomolas/iStockphoto

6.4 Veränderung der Angebotsseite

Chinesische Hersteller von 5G-Technik sehen sich derzeit mit **Exportbeschränkungen** konfrontiert, die von der US-Regierung für Betriebsmittel verhängt wurden, die mit US-Technik entwickelt und produziert wurden (zum Beispiel Halbleiter oder Googles Android-Software[98]). Diese Beschränkungen beeinträchtigen die Möglichkeiten chinesischer Hersteller, 5G-Komponenten zu produzieren, erheblich. Sie führen auch zu Zweifeln an der Qualität der Produkte, die geliefert werden können, wenn die Komponenten des erstbesten Lieferanten fehlen. Wenn die Lösung darin besteht, US-Technik wie Mikrochips durch chinesische Technik zu ersetzen, wird dies das Vertrauen in solche Netzwerkkomponenten im Westen noch weiter verschlechtern.

Japanische und südkoreanische Chips sind potenziell **zweitbeste Substitute**, wenn ihnen nicht ähnliche Beschränkungen auferlegt werden. So wurden z. B. Unternehmen, die Produkte an Chinas wichtigsten Chiphersteller, die Semiconductor Manufacturing International Corporation (SMIC), liefern, vor kurzem vom US-Handelsministerium darüber informiert, dass die Fortsetzung ihrer Tätigkeit ein „inakzeptables Risiko" darstelle, da solche Produkte für „militärische Endzwecke" umgeleitet würden[99], und es wurde ihnen abgeraten, ihre Geschäftsbeziehungen aufrechtzuerhalten.

96 Bundesrechnungshof (2017).
97 Bundesgesetzblatt (2020).
98 Globaltrademag.com (2020).
99 Financial Times (2020a).

Ein anderer Aspekt im Zusammenhang mit dem Anbieterwettbewerb betrifft die **Lock-in-Effekte** von Lieferanten (Eigentümern, Kunden). Zu den möglichen Ursachen von Lock-ins gehören unfaire Preispraktiken. Europäische und südkoreanische Wettbewerber werfen Huawei vor, Produkte unter dem Einkaufspreis zu verkaufen.[100] Dieses **Dumping** kann für ein gewinnorientiert arbeitendes Unternehmen nur als kurz- bis mittelfristige strategische Maßnahme sinnvoll sein, um Wettbewerber aus dem Markt zu drängen. Es ist nur bei fehlenden Sanktionen der Wettbewerbsbehörden und bei ausreichendem finanziellem Durchhaltevermögen oder versteckten Subventionen des Heimatstaates möglich.

Die versteckten Kosten, die entstehen, wenn man Produkte von einem Anbieter bezieht, der seine Konkurrenten durch Dumping aus dem Markt drängt, werden typischerweise erst nach einiger Zeit sichtbar. Wenn die verbleibenden westlichen Anbieter von Netzwerktechnik aus dem Geschäft aussteigen, werden wir für die kritische Infrastruktur und für die Handhabung unserer Daten vollständig von chinesischer Technik abhängig sein. Dieser Aspekt ist von besonderer Bedeutung, wenn man über 5G hinaus in die Zukunft zu 6G blickt.

Wie bereits in anderen Branchen erlebt, werden die Preise wieder steigen, sobald Konkurrenten aus dem Westen den Markt verlassen. Allerdings ist der (Wieder-)Einstieg in den Markt schwierig und erfordert viel Aufwand und Eigenkapital. Die wirtschaftliche Rendite aus der Produktion von Mobilfunknetzen wird wahrscheinlich vollständig in China landen.

Der fehlende Wettbewerbsdruck in Kombination mit der dann bereits bewiesenen Bereitschaft, ihre Marktmacht zu missbrauchen, wird zu strukturellen finanziellen Nachteilen für Mobilfunknetzbetreiber und letztlich für die Verbraucher führen, da höhere Kosten höhere Preisen bedeuten. In einem Zweitrundeneffekt wird der nicht-vertrauenswürdige Anbieter einen Anreiz haben, die Preise über die Anschaffungskosten hinaus anzuheben, aus zwei Beweggründen:

a. Motivation: Die Dumpingphase war für den Verkäufer kostspielig (es sei denn, dies wurde vom Heimatstaat kompensiert).

b. Opportunität: Die Preiselastizität der Nachfrage ist höher als in einem Wettbewerbsmarkt, da Mobilfunknetzbetreiber kaum noch die Wahl haben, von welchem Anbieter sie beziehen wollen.

Eine weitere Frage im Zusammenhang mit Lock-in bezieht sich auf entgangene Gewinne bei der Verhandlungsmacht und deren nachgelagerte Auswirkungen. Mit der globalen Beschaffung der Mobilfunknetzbetreiber und der bevorstehenden Einführung von OpenRAN sollte sich die Marktmacht zugunsten der Betreiber verschieben. Dieser wirtschaftliche Vorteil, der sich aus einem kontinuierlichen oder zumindest periodisch wiederkehrenden Wettbewerb ergibt, entfällt jedoch, wenn sich ein Netzanbieter nicht an OpenRAN beteiligt.

6.4.1 OpenRan und die Auswirkungen auf das Angebot

Die Einschränkung der Wahlmöglichkeiten von Mobilfunknetzbetreibern bezüglich der Palette potenzieller Anbieter von 5G-Kommunikationsnetzausrüstung stößt auf Vorbehalte von Wettbewerbshütern hinsichtlich einer zu hohen Marktkonzentration auf der Angebotsseite. Diese Einwände könnten jedoch angesichts der jüngsten Marktentwicklungen und Innovationen kurzsichtig sein.

In den vorherigen Mobilfunknetz-Generationen, einschließlich 4G, waren herstellereigene Hardware-Komponenten nicht mit denen von Konkurrenzanbietern kompatibel. Dies machte den Wechsel zu einem anderen Anbieter zu einer sehr kostspieligen Entscheidung für Mobilfunknetzbetreiber. Selbst wenn sich ein Betreiber also im Kern für einen Anbieter oder eine Gruppe von Anbietern entschied, hatte er nicht die Möglichkeit, seine Funknetzwerke auf der Benutzerzugangsebene einfach und bedarfsgerecht zu skalieren, wenn er mehrere Anbieter einsetzte. Ein Anbieter, der RAN-Implementierungen mit eigener Technologie zu niedrigen Preisen anbietet, bewirkt, dass andere Anbieter vom Wettbewerb in großen Teilen des Zugangsnetzes ausgeschlossen werden, es sei denn, der Käufer (oft ein Mobilfunknetzbetreiber) ersetzt den größten Teil davon auf einen Schlag.

OpenRAN ändert diese Marktdynamik und hat dies bereits getan. Betreiber, die sich für die Nutzung

100 Washington Post (2019) und Strand Consult (2019).

von OpenRAN entscheiden, können dann ihre Hardware aus einer viel größeren Gruppe von Anbietern auswählen, anstatt gezwungen zu sein, bestimmte herstellerspezifische Produkte zu verwenden. Mobilfunknetzbetreiber werden in der Lage sein, **Commercial-of-the-shelf (COTS)**-Komponenten zu verwenden, da Produkte verschiedener Hersteller auf der gleichen Netzwerkebene und sogar am gleichen Standort eingesetzt werden können. Dies wird **neutrales Hosting** und andere Arten der gemeinsamen Nutzung von Infrastruktur eröffnen, die die Kosten für die Bereitstellung senken und neue Anwendungsfälle ermöglichen, die das Wachstum von Verbraucherdiensten und kleinen Unternehmen fördern. Die Marktmacht etablierter Anbieter wird zugunsten des Wettbewerbs und des Verbraucherwohls deutlich abnehmen, und es werden viele neue Arten von sicheren, standardbasierten Netzwerken entstehen.

Die beiden chinesischen Anbieter zeichnen sich bisher nicht durch eine kommunizierte Bereitschaft zur Teilnahme an der OpenRAN-Initiative aus. Stattdessen konzentrieren sie sich darauf, aufgrund der angeblichen Bedenken hinsichtlich Leistung, Skalierbarkeit und betrieblicher Komplexität dagegen zu lobbyieren. Sie drängen weiterhin auf ihre firmeneigenen Hardware- und Verbindungsstandards in ihren 5G-Angeboten, was wiederum den Übergang zu einem offenen Markt für Verbindungen in Zukunft sehr viel schwieriger machen wird.

Diese angeblichen Bedenken haben sich bei den ersten Implementierungen nicht bewahrheitet, da Vodafone OpenRAN-basierte 4G- und 5G-Versuche in Großbritannien und anderswo durchführt. Rakuten führt bekanntermaßen groß angelegte Multi-Vendor-Implementierungen in Japan mit OpenRAN durch. Tatsächlich stellt Rakuten fest, ihr Netzwerk *"has been built 40% cheaper than would have been possible using traditional vendors and which is running at 30% below the expected operating costs of running a traditional mobile network".*[101] Dies hat europäische Partner wie Telefonica dazu inspiriert, eine Absichtserklärung mit ihnen zu unterzeichnen, um die Entwicklung und den Einsatz von OpenRAN-basierter 5G-Infrastruktur voranzutreiben.

Auch europäische und koreanische Anbieter nehmen eine offenere und proaktivere Haltung ein und tragen aktiv zur Entwicklung und schnellen Einführung von Netzwerken auf Basis von OpenRAN-Standards bei. Die versteckten Kosten der Einbindung von nicht-vertrauenswürdigen Anbietern beziehen sich daher in diesem Zusammenhang auf die entgangene Flexibilität, den Wettbewerb und das Wohl der Verbraucher. Es ist auch möglich, dass OpenRAN den **Erstanbietervorteil** deutlich verringert, da es erst in Kürze allgemein verfügbar wird.

6.4.2 Marktstrukturen

Ein weiterer Aspekt beim Wettbewerb auf den 5G-Netzmärkten ist die allgemeine Marktstruktur. Der Telekommunikationsausrüstungsmarkt in den meisten westeuropäischen Ländern kann durch eine Oligopol-Oligopsy-Struktur charakterisiert werden. Die akademische Verhandlungsliteratur suggeriert für einen solchen Markt immer noch ein effizientes Ergebnis[102] und lässt vermuten, dass die potenzielle Beeinträchtigung des Wettbewerbs durch den Ausschluss von nicht-vertrauenswürdigen Anbietern vernachlässigbar ist.

Da die Anbieter von Telekommunikationsnetzwerkausrüstung außerdem relativ hohe Bruttomargen beim Verkauf erzielen, haben sie im Falle einer Reduzierung der Verkaufsmengen auch viel zu verlieren. Wendet man Werkzeuge der kritischen Verlustanalyse an und berechnet, dass die Anbieter in diesem Fall etwa 13 % ihres Umsatzes verlieren würden, **erhöhen sie die Preise** um lediglich fünf %.[103] Da die Abnehmer - also die Mobilfunknetzbetreiber - in den meisten europäischen Ländern recht konzentriert sind und Alles-oder-Nichts-Angebote unter solchen Umständen eine typische Verhandlungstaktik sind, ist die Gefahr von Preiserhöhungen nach einer Ausschlussentscheidung eher gering.

Auf der Anbieterseite haben die beiden chinesischen Anbieter einen Marktanteil von 48 % am Markt für 4G-RAN-Ausrüstung in ganz Europa. In drei Ländern wird das 4G-RAN komplett von Huawei und ZTE ausgestattet (Belgien, Zypern und auf den dänischen Färöer-Inseln). In 15 Ländern liegt ihr Marktanteil bei über 50 % (z. B. Deutschland, Griechenland und Italien).[104]

101 Le Maistre (2020).
102 z.B. Baldwin & Krugman (1988).
103 Wagener (2020).
104 Strand Consult (2020).

Zudem scheinen keine **Verzögerungen beim Aufbau** von 5G-Netzen in jenen Ländern eingetreten zu sein, die nicht-vertrauenswürdige Anbieter de jure oder de facto als Netzwerkausrüster ausgeschlossen haben. Durchgeprüfte Quartals- und Jahresberichte, die bei der US-Börsenaufsichtsbehörde eingereicht wurden, erwähnen keine Verzögerungen oder erhöhte Anschaffungskosten.[105]

Dieser Befund deckt sich mit unseren Erkenntnissen aus Interviews mit westlichen Anbietern. Ein Beispiel ist der Aufbau eines von Ericsson eingerichteten 5G-Netzes in Dänemark innerhalb von zehn Monaten, trotz der Einschränkungen durch die Corona-Pandemie. Einer der dänischen Telekommunikationskonzerne, TDC, entschied sich im Frühjahr 2019 aus Sicherheitsgründen gegen einen Kauf bei Huawei. Befürchtungen, dass diese Entscheidung zu erheblichen Verzögerungen beim Ausbau des 5G-Netzes führen würde, traten nicht nur nicht ein, sondern der letztlich ausgewählte europäische Anbieter konnte den Ausbau trotz Pandemiebedingungen im Jahr 2020 drei Monate schneller als ursprünglich geplant abschließen.[106] Das heißt nicht, dass es keine Verzögerungen bei der Einführung von 5G gibt. Diese sind jedoch meist auf politische oder rechtliche Probleme zurückzuführen (zum Beispiel zwischen etablierten 4G-Netzbetreibern und potenziellen Markteinsteigern).

6.5 Produktivitätskosten

Die versteckten Kosten die durch nicht-vertrauenswürdige Anbieter entstehen, drehen sich auch um entgangene Produktivitätsgewinne, Stagnation oder sogar Produktivitätsverluste - mit anderen Worten: **Opportunitätskosten.** Die zugrundeliegenden Ursachen beziehen sich auf die unvollständige Ausschöpfung des Potenzials von 5G aufgrund von Sicherheitsbedenken der Nutzer.

Diese Bedenken gibt es in vielen Unternehmen bereits, zum Beispiel in Bezug auf Cloud-Computing oder die Anbindung des Produktionsprozesses an das Internet überhaupt. Risikoscheue und Sicherheitsbedenken können leicht zu Produktivitätsverlusten führen. Insbesondere Kleinst-, Klein- und mittelständische Unternehmen, die nicht über eine eigene IT-Sicherheitsabteilung und Netzwerksicherheitsressourcen verfügen und denen es an hausinterner Verschlüsselungskompetenz mangelt, neigen dazu, die Tendenz zur Lokalisierung von Daten fortzusetzen oder wiederzugewinnen, anstatt die Möglichkeiten cloudbasierter Prozesse und Produkte zu nutzen. Dies verhindert die Nutzung von nahtlosen und reibungsarmen Kollaborationswerkzeugen und behindert damit die Effizienz des Einsatzes von Arbeitskräften und Zeit sowie von Ressourcen. Redundante und veraltete Technik muss zudem gewartet werden. Bildlich gesprochen geht es um das Mechatronik-Unternehmen mit eigenem Server im Keller und ohne Cloud-Backup.

Laut einer Studie von Bitkom Research, in der 553 Unternehmen befragt wurden, nutzten 73 % Cloud Computing in 2018.[107] Allerdings machen sich 73 % der Nicht-Nutzer Sorgen um die Sicherheit ihrer Daten und befürchten einen unbefugten Zugriff auf sensible Unternehmensdaten. 64 % befürchten einen möglichen Datenverlust und weitere 51 % vermuten eine unklare Rechtslage. Wenn Sicherheitsbedenken einige Marktteilnehmer daran zweifeln lassen, dass der Einsatz digitaler innovativer Technik sie oder ihre Daten einem unüberschaubaren Risiko von Datendiebstahl und Spionage aussetzt, wird auf potenzielles Wachstum verzichtet. Diese entgangenen potenziellen Produktivitätsgewinne sind letztlich die Kosten eines mangelnden Vertrauens in mobile Netzwerke mit nicht-vertrauenswürdiger Technik.

Die weltweite Debatte über die chinesische Technik in 5G-Netzen und die Tatsache, dass bereits bedeutende verbündete Länder beschlossen haben, diese Technik in ihren Netzen zu verhindern oder auslaufen zu lassen, wird sicherlich die Entscheidungsträger auf Unternehmensebene beeinflussen, ob sie 5G-Anwendungen in ihrem Unternehmen einsetzen werden.

Ein weiterer Punkt sind versteckte Kosten, die durch Interoperabilitäts- und Sicherheitsprobleme entstehen. Wie bereits erwähnt, wird die Notwendigkeit, mehr Sicherheitstechnik in vertrauensunwürdige 5G-Netzwerke einzubinden, um das fehlende Vertrauen

105 Strand Consult (2020).
106 Ericsson (2020b).
107 KPMG (2019).

in die verwendete Technik (teilweise) auszugleichen, die Geschwindigkeit des Netzwerks verlangsamen. Doch der Geschwindigkeitsgewinn ist ein großer Teil des Produktivitätsgewinns beim Übergang von 4G auf 5G. Das volle Potenzial oder die Geschwindigkeit von 5G nicht ausschöpfen zu können, sind Kosten, die direkt mit dem Grad des Vertrauens in die verwendete Technologie zusammenhängen.

Ein weiterer Aspekt, der eng mit den zusätzlichen Sicherheitsmaßnahmen verbunden ist, ist die Zunahme der Komplexität im Projektmanagement. Sich um die verschiedenen technischen und verwaltungstechnischen Sicherheitsaspekte kümmern und diese koordinieren zu müssen, nimmt der Unternehmensleitung Zeit und Energie ab und verursacht Kosten. Das Management könnte das Gefühl haben, sich entscheiden zu müssen, ob es den Wettbewerbsvorteil des Unternehmens aufgrund eines zu hohen Risikos verliert, indem es die Kronjuwelen an ein nicht-vertrauenswürdiges Netzwerk preisgibt, oder ob es seinen Vorteil verliert, weil die Konkurrenz durch die Digitalisierung aufholt, vor der es selbst zurückschreckt. Auch hier gilt, dass die beschriebene Herausforderung nicht nur für 5G oder nicht-vertrauenswürdige Anbieter gilt, sondern in zunehmendem Maße für das mangelnde Vertrauen in die neuen Netzwerke.

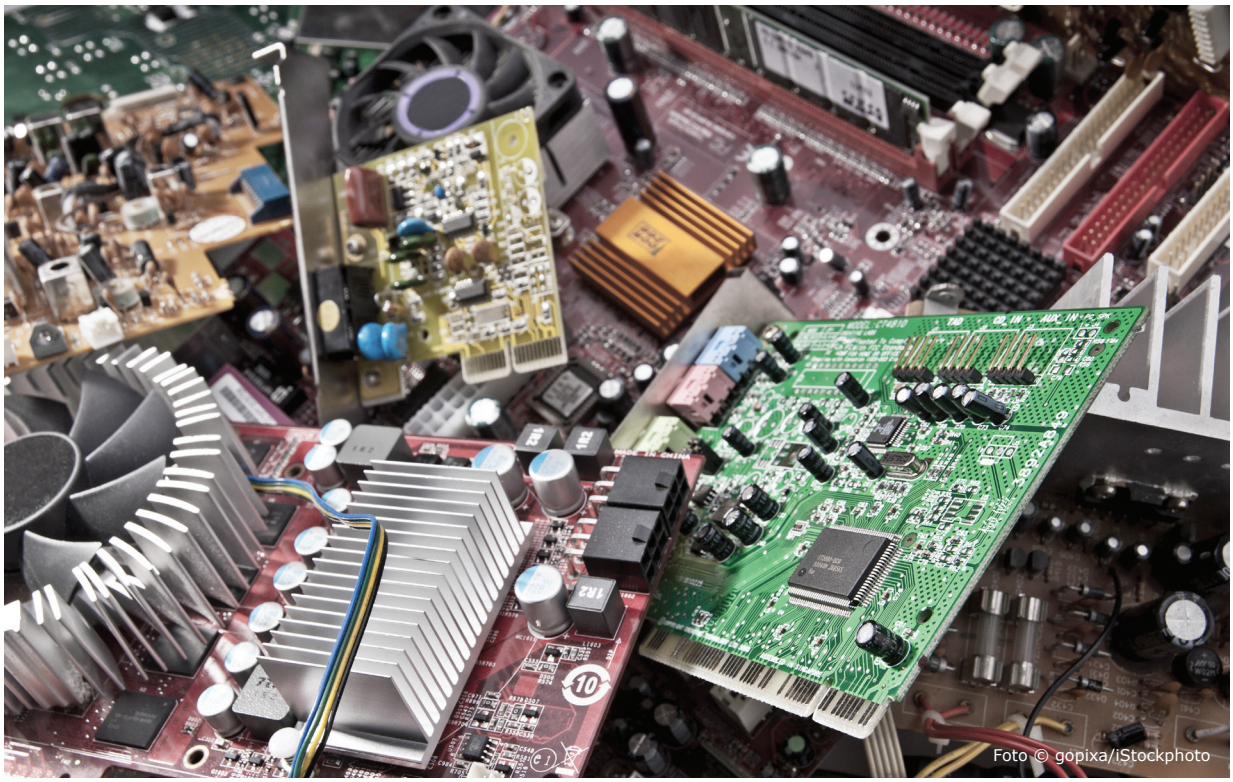


Foto © gopixa/iStockphoto

7 KOSTEN FÜR DIE REAKTION NACH EINEM STÖRFALL

Sollte sich herausstellen, das politische Entscheidungsträger und Mobilfunknetzbetreiber falsches Vertrauen in den Anbieter der 5G-Technik gesetzt haben und die Gewissheit wächst, dass der Anbieter mit einem Widersacher zusammengearbeitet hat, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder eines Netzwerks zu verletzen, muss eine politische, organisatorische und technische Reaktion folgen. Alle drei sind kostspielig. Sanktionen, Embargos oder militärische Maßnahmen haben einen Preis, den eine Gesellschaft entweder bereit sein muss zu zahlen, oder sie opfert ihre eigene Souveränität. Diese politischen Kosten sollen hier aber nicht weiter ausdifferenziert werden.

Der erste Schritt jeder Reaktion muss eine gründliche Untersuchung der Angriffsstrategie sein und sollte die Zuordnung beinhalten, wer der Angreifer war, wer der Auftraggeber des Angreifers ist und wer von dem Angriff profitiert (7.1). Ein zweiter Schritt besteht aus einer Schadensbeurteilung, die zusätzliche knappe Ressourcen erfordert. Der dritte Schritt ist die Vermeidung, dass sich ein ähnliches Ereignis jemals wiederholt (7.2). Hier hat der Zeitfaktor einen großen Einfluss auf die Kosten. Sobald das Vertrauen verletzt wurde, wird der nicht-vertrauenswürdige Anbieter zu einem böswilligen Anbieter, der letztlich nicht mehr Teil einer kritischen Infrastruktur sein kann (7.3). Heißt das aber, dass die Infrastruktur nicht mehr genutzt werden darf, bis der nicht-vertrauenswürdige Anbieter ersetzt ist? Oder kann das Netzwerk so lange betrieben werden, bis die Technik am Ende ihrer Abschreibungszeit ausläuft?

7.1 Untersuchung und Zuordnung

Die Untersuchung von Ereignissen wie z. B. Cyberangriffe ist als komplexe Disziplin anerkannt. 5G-Netzwerke stellen neue und wichtige Herausforderungen für traditionelle forensische Ansätze dar. So werden beispielsweise die eindeutigen Kennungen, die Smartphones und verbundene Geräte in aktuellen Telekommunikationsnetzen verbinden, durch temporäre Zertifikate ersetzt, die von jeder Antenne erneuert werden. Darüber hinaus werden Standard-Forensik-Techniken und -Richtlinien wie ISO/IEC 27037:2012 oder NIST SP 800-101 eher an der hochkomplexen und dynamischen Natur von 5G-Netzwerken scheitern.

Der Standard Ablauf für die Untersuchung[108] ist weniger effektiv und praktisch, wenn die von Angriffen und/oder Angreifern hinterlassenen Beweise über verschiedene und fragmentierte Domänen und Standorte mit potenziell unterschiedlichen und widersprüchlichen Vorschriften verteilt sind, was die Sammlung und Verarbeitung von Beweisen erschwert. Überwachungswerkzeugen fehlen geeignete Lösungen für die forensische Analyse, wenn die zu sammelnden und zu verarbeitenden Daten Hunderte oder Tausende von Geräten umfassen. Klassische Security-Information-and-Event Management-(SIEM)-Lösungen sind nicht an die Verarbeitung von 5G-Daten angepasst und verfügen nur über begrenzte Fähigkeiten zur Unterstützung der nachträglichen Zuordnung der Haftung.

Digitale Ermittlungen in 5G-Netzwerken müssen disziplinübergreifend erfolgen und die Strafverfolgungsbehörden aktiv einbeziehen, um einen sicheren Zugriff, die Erfassung und Übermittlung von Beweisen für Cyberangriffe zu gewährleisten. Eine solche Zusammenarbeit erfordert ein hohes Maß an Vertrauen zwischen den verschiedenen Beteiligten. Bei Vorhandensein von nicht-vertrauenswürdigen Geräten können die vom Gerätehersteller bereitgestellten Tools und Beweise die Ergebnisse und Erkenntnisse der Untersuchung schwächen.

7.2 Schadensbewertung

Die in der Regel fehlerhafte Bewertung des Schadens eines Cybervorfalls rührt von der Art und der Sensibilität der Informationen her, die Unternehmen preisgeben müssen, nämlich den Diebstahl von persönlichen Daten, Bankverbindungen oder medizinischen Informationen. Infolgedessen beschränkt sich die Berechnung der Kosten eines Angriffs in der Regel auf die Spitze des Eisbergs und berücksichtigt nur die Kosten, die mit Kundeninformationen, Kreditüberwachung, Rechtsstreitigkeiten und regulatorischen Sanktionen zusammenhängen.

5G wird eine solche Bewertung höchstwahrscheinlich noch komplizierter machen, da ein einzelner Angriff mehrere kaskadierende und sich ausbreitende Auswirkungen haben kann, die zu anderen Zielen als dem einfachen Datendiebstahl führen. In solchen Fällen können die Auswirkungen weitreichender sein, und die Kosten sind besonders schwer zu bewerten. Denken Sie nur an die jüngsten (2019) Ransomware-Angriffe auf mehr als 23 Kommunalverwaltungen in Texas.[109] Solche Angriffe machen stadtweite smarte Dienste für die Bürger nicht mehr verfügbar und verursachen erhebliche Schäden für lokale Unternehmen

Bestehende Rahmenwerke zur Schadensbeurteilung, wie die in den ISO-Normen (27000 oder 21434) vorgeschlagenen, definieren Schaden als *"adverse consequence or undesirable result due to the compromise of cybersecurity property (or properties) of an asset, or of a group of assets"*. Der Schaden bezieht sich also nur auf das befürchtete Szenario, das durch Sicherheitsmaßnahmen verhindert oder gemildert werden soll. Die Quantifizierung des Schadens erfolgt in der Regel durch die Verwendung der Auswirkungsanalyse, die darauf abzielt, das Ausmaß des Schadens aufgrund der Kompromittierung einer der Sicherheitseigenschaften abzuschätzen. Da 5G sowohl die digitale als auch die physische Welt umspannt, sind wir der Meinung, dass die Auswirkungen in Bezug auf die vier Kernkategorien **Sicherheit, Finanzen, Betrieb und Datenschutz** bewertet werden müssen, wie in ISO 26262 definiert.

108 Vorbereitung, Datenidentifikation, Datenhaltung, Datenprüfung, Untersuchung und Bericht.

109 Laut NIST, „Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management." https://www.nist.gov/el/cyber-physical-systems.

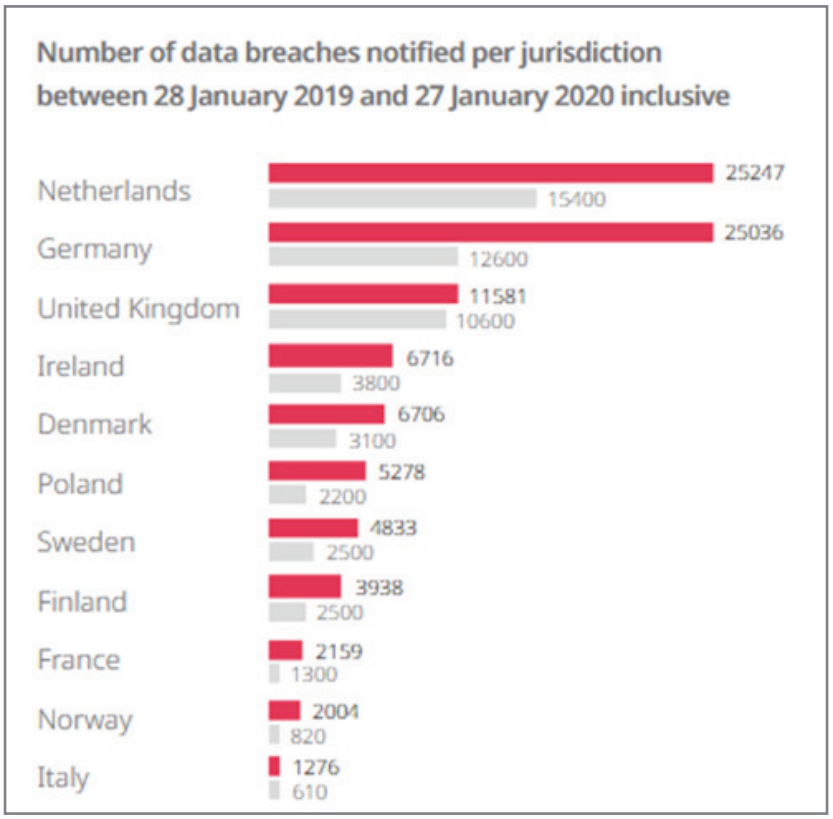
Sicherheit und Schutz sind zwei unterschiedliche Konzepte, die in der Regel aneinander gekoppelt sind. Der kritischste Anwendungsbereich, in dem sich Sicherheitsrisiken heute auswirken, ist der Kontext von Cyber-Physical Systems (CPS),[110] wie sie in der digitalen Fertigung (Industrie 4.0) oder in intelligenten Transportsystemen eingesetzt werden. Die meisten kritischen CPS-Systeme implementieren in der Regel sicherheitsgerichtete Systeme (Safety Instrumented Systems, SIS), die Steuerungsfunktionen ausführen, um einen sicheren Betrieb aufrechtzuerhalten und minimale Schäden für Mensch und Umwelt zu gewährleisten. Wenn sie jedoch mit 5G verbunden sind, könnten solche Systeme durch einen böswilligen Akteur außer Betrieb gesetzt werden und schwere Unfälle verursachen.

Darüber hinaus wird die Industrie 5.0 durch die Zusammenarbeit zwischen Menschen und Maschinen gekennzeichnet sein, mit dem Ziel, der Produktion einen Mehrwert zu verleihen, indem personalisierte Produkte geschaffen werden, die den Anforderungen der Kunden entsprechen. Die Zusammenarbeit von Menschen mit fortschrittlichen Maschinen, zum Beispiel kollaborierenden Robotern, stellt neue Herausforderungen an die Prozesssicherheit. Die ISO 10218 ist die relevanteste Normenreihe, in der Sicherheitsanforderungen für kollaborierende Roboter definiert sind. Bedrohungen, die von nicht-vertrauenswürdigen 5G-Geräten ausgehen könnten, stellen jedoch die Wirksamkeit und Praktikabilität dieser Standards in Frage.

Der **finanzielle** Schaden von Vorfällen kann Kosten umfassen, die in verschiedenen Bereichen entstehen. Rechtskosten, Haftungen und Bußgelder, die durch den Verlust sensibler Kundendaten entstehen, Umsatzeinbußen durch Produktfälschungen von Mitbewerbern, zusätzlicher Arbeitsaufwand durch Change Management und Behelfslösungen sowie Ad-hoc-Anschaffungen von Backup- und Side-Track-Informationstechnologie sind nur einige der Kostenpositionen, die betroffene Unternehmen belasten. Der finanzielle Schaden, der durch Datenschutzverletzungen entsteht, ist schwer zu beziffern. IBM hat im November 2020 einen Bericht zu diesem Thema veröffentlicht[111]. Basierend auf diesem Bericht bewerten wir in den jeweiligen Länderstudien die Kosten, die auf nicht- vertrauenswürdige Anbieter in 5G zurückzuführen sind.

IBM hat, in dem oben erwähnten Bericht, den durchschnittlichen Schaden einer Datenschutzverletzung pro Land berechnet. In Abbildung 3 zeigen wir die Anzahl der gemeldeten Verstöße pro Land im Jahr 2019. Auffällig ist der große Unterschied zwischen den Ländern, der auf unterschiedliche nationale Regelungen zur Meldepflicht zurückzuführen ist. Die unrealistisch niedrigen Zahlen für Frankreich und Italien schränken die Aussagekraft für diese Länder ein und erfordern zusätzliche Annahmen.

Abbildung 3



Quelle: DLA Piper (2020).

110 Vgl. Bischoff (2020).
111 IBM (2020).

Der Angriffsvektor einer Attacke kann vielfältig sein. Wir betrachten daher den Anteil der Daten, die durch 5G-Netzwerke übertragen werden, und den Anteil der nicht-vertrauenswürdigen Technologie in diesen Netzwerken.[112] Letztlich sieht die Formel für die Kosten von Datenschutzverletzungen aufgrund von nicht-vertrauenswürdigen Anbietern in 5G-Netzwerken so aus:

$$pca_t^{br\ 5G\ ctry} = \left(c_{t-1}^{br\ ctry} * \frac{1}{3} * r_t^{cc\ ctry} + c_{t-1}^{br\ ctry}\right) * \sum_{mno=1}^{n} \left(dsh_t^{mno\ ud\ ctry} * msh_t^{mno\ m\ ctry}\right) * \left(pen_{t-1}^{5G\ ctry} * \left(1 - obs_t^{5G\ ctry}\right)\right) * n_t^{br\ ctry}$$

mit:

$pca_t^{br\ 5G\ ctry}$ = geschätzter Anteil der aggregierten Kosten der Datenschutzverletzungen, die auf Sicherheitsprobleme von 5G zurückzuführen sind, im jeweiligen Land im Zeitabschnitt Jahr t

$c_{t-1}^{br\ ctry}$ (letztes Jahr) = Gesamtkosten einer Sicherheitsverletzung, im jeweiligen Land im Zeitraum Jahr t-1

$r_t^{cc\ ctry}$ = Anstieg der Internetkriminalität, im jeweiligen Land im Zeitraum Jahr t

$dsh_t^{mno\ ud\ ctry}$ = Prozentsatz der nicht-vertrauenswürdigen 5G-Geräte, die in den Mobilfunknetzbetreibern aktiv sind, im jeweiligen Land im Zeitraum Jahr t

$msh_t^{mno\ m\ ctry}$ = Mobilfunknetzbetreiber-Marktanteil im jeweiligen Land, im jeweiligen Land im Zeitabschnitt Jahr t

$pen_{t-1}^{5G\ ctry}$ = Schätzung der Verbreitung von 5G im Vergleich zum globalen Verkehr, im jeweiligen Land im Zeitraum Jahr t-1 (letztes Jahr)

$obs_t^{5G\ ctry}$ = Obsoleszenz in % der vorhandenen 5G-Endgeräte (Substitutionsrate), im jeweiligen Land im Zeitabschnitt Jahr t

$n_t^{br\ ctry}$ = Gesamtzahl der Verstöße, im jeweiligen Land im Zeitraum Jahr t

Wenn die Angriffe auf nicht-vertrauenswürdige Anbieter zurückzuführen sind, wird der Steuerzahler die Kosten für den dann unvermeidlichen Prozess der Anpassung der Regulierung tragen müssen. Im Falle eines reaktiven „Rip and Replace" nach einem Vorfall (mehr dazu unten in Abschnitt 7.3) wären die Kosten weitaus höher als bei einer präventiven Abschaltung. Während Letzteres vom Mobilfunknetzbetreiber in enger Abstimmung mit den vertrauenswürdigen Anbietern geplant, kontrolliert und verwaltet werden kann, wird Ersteres überraschend und als bekannte Unbekannte eintreten. Zweifellos wird ein plötzliches „Rip and Replace" deutlich kostspieliger, da ein neuer Anbieter mit Zugangskapazität zur Verfügung stehen muss.

Natürlich hängt der Umfang der zusätzlichen Kosten von der Größe des Projekts ab. Während ein kleineres

112 Die drei Phasen des Datenlebenszyklus sind (1) Ingestion (Erfassung von lokalen Sensoren), (2) Daten in Transit und (3) Data im Ruhezustand. Lord (2019).

Netzwerk (in einem kleineren Land) vielleicht in die Pläne eines Netzwerkanbieters gequetscht werden kann, wird ein großer zusätzlicher Auftrag die Kapazitäten an ihre Grenzen bringen. Die notwendige Verfügbarkeit von qualifiziertem Personal scheint uns in diesem Szenario der größte Kostentreiber zu sein.

Auf **operativer** Ebene fühlt es sich so an, als ob wir bereits von hypervernetzten Geräten überflutet werden, die einen massiven Datenfluss erzeugen. 5G wird diese Konnektivität noch beschleunigen. Dieser signifikante Anstieg der Anzahl verbundener Geräte wird unwiderruflich zu einer Zunahme und Beschleunigung von Cyberangriffen über 5G-Netzwerke führen. In der Industrie 5.0 werden beispielsweise Daten am „Rand" von Sensoren des industriellen Internet der Dinge generiert, die in der Produktionshalle verteilt sind, und entlang einer relativ komplexen Kette von „Beteiligten" weitergeleitet. In einem solch komplexen und mehrstufigen Kontext ist das Vertrauen in die Daten und das Transportnetzwerk ein Schlüsselfaktor. Eine potenziell nicht-vertrauenswürdige Netzwerkebene bedeutet im Allgemeinen einen Vertrauensverlust in das gesamte industrielle Steuerungssystem. Private Netzwerke sind nicht der EU-Toolbox unterworfen und können ohne rechtliche Einschränkungen installiert werden. Zudem sind für den Industriebetrieb Rip-and-Replace-Kosten oft unbezahlbar, da sie meist eine Unterbrechung des Betriebs und Unterbrechungen der Produktivität erfordern.

Datenschutz bezieht sich auf den Schaden, der nach der Aufdeckung oder dem Durchsickern digitaler Daten, die private Informationen enthalten, entsteht. Von dieser Schadenskategorie sind verschiedene Instanzen betroffen, vom Unternehmen, das die Daten durchsickern ließ, bis hin zum Endnutzer und Kunden, der von den offengelegten Daten betroffen ist. Die erste Kategorie (d. h. Unternehmen oder Organisationen) fällt automatisch unter die bestehenden allgemeinen rechtlichen Rahmenbedingungen. Wenn Daten europäischer Bürger betroffen sind, sieht die DGVO Geldstrafen von bis zu 4 % des Jahresumsatzes oder 20 Mio. Euro vor, je nachdem, welcher Betrag höher ist. Unternehmen wie British Airways (204,6 Mio. Euro), H&M (35,3 Mio. Euro), Google (ca. 50 Mio. Euro) oder der italienische Telekommunikationsbetreiber TIM (ca. 27,8 Mio. Euro) haben bereits Bußgeldbescheide ihrer jeweiligen Datenschutzbehörden erhalten oder sogar bezahlt.

Zusätzlich zu den bereits erwähnten Bußgeldern sind die gesellschaftlichen und indirekten wirtschaftlichen Risiken über Reputationsschäden zu groß, um sie zu ignorieren. Studien zeigen, dass Unternehmen, die von einer Datenschutzverletzung betroffen sind, nach nur einem Jahr an der NASDAQ eine um durchschnittlich 3,7 % schlechtere Performance aufweisen.[113] Die Opfer (65 %) berichten von einem Vertrauensverlust in ein Unternehmen und 85 % geben an, dass sie wahrscheinlich andere über ihre negativen Erfahrungen informieren werden.[114]

7.3 Rip-and-Replace

Ein Hauptargument derjenigen, die sich gegen ein Verbot von nicht-vertrauenswürdigen Anbietern in 5G-Netzen aussprechen, sind die damit verbundenen Kosten, die zweifellos entstehen, wenn bereits installierte vertrauensunwürdige Technik entfernt werden muss und wenn alte Verträge gekündigt und neue ausgehandelt werden müssen. All dies verursacht versunkene Kosten. So behauptet die Deutsche Telekom z.B., dass die Gesamtkosten drei Milliarden Euro betragen würden, wenn sie Huawei nicht als Anbieter für ihr 5G-Netz nutzen dürfte und die bestehende Technologie von Huawei aus ihrem 4G-Netz ersetzen müsste.[115] Diese Kosten würden zunächst auf die Mobilfunknetzbetreiber fallen, aber auch (zumindest in Teilen) an deren Kunden weitergegeben.

Die Beschaffung durch vertrauenswürdige Anbieter würde auch bedeuten, dass die Preise nicht mehr den zuvor beschriebenen „Rabatt" enthalten, den nicht-vertrauenswürdige Anbieter ihren Kunden gewähren. Die mit der Unzuverlässigkeit verbundenen externen Kosten, die von den 5G-Kunden getragen wurden, würden nun auf die Mobilfunknetzbetreiber fallen. Diese Kosten können und werden aber letztlich an die Kunden weitergegeben.

Letztlich ist das Rip-and-Replace-Argument der Mobilfunknetzbetreiber eine Wette darauf, dass China die Chancen nicht ausnutzt, die sich mit dem Zugang zu westlichen 5G-Netzen durch politisch kontrollierte Unternehmen über die Lebensdauer

113 Ponemon Institute (2017).
114 Winder (2019).
115 Handelsblatt (2020).

der nicht-vertrauenswürdigen Technologie ergeben. Oder, falls dies doch erfolgt, dass die Ausnutzung zumindest unerkannt bleibt.

Sollten die Mobilfunknetzbetreiber diese Wette verlieren und die „Smoking Gun" von den Behörden, Cyberexperten oder von Kunden selbst entdeckt werden, wird der Reputationsschaden für die Betreiber enorm sein. Alarmierte Kunden werden den Anbieter wechseln und es ist wahrscheinlich, dass die Regulierungsbehörden einen schnellen Austausch der (nunmehr offensichtlich) bösartigen Technik fordern werden. Wenn sich dieses Szenario als realistisch erweist, ist es nur eine Frage des Zeitpunkts, wann die Kosten für Rip-and-Replace anfallen werden. Zweifellos werden die Kosten für der Technikaustausch in einem späteren Lebenszyklus von 5G teurer sein als zu einem früheren Zeitpunkt, zu dem 3G / UMTS noch in Betrieb ist und Investitionen in die Verbesserung von 4G-Netzen noch stattfinden.

Wenn man nicht an dieses Szenario glaubt, sollte man sich bereits bekannte und gut recherchierte Fälle wie bei der Afrikanischen Union (AU) oder Papua-Neuguinea (PNG) ansehen.

Im ersten Fall hat China den neuen Hauptsitz der AU in Addis Abeba als Geschenk an die multinationale Organisation gebaut und ausgestattet. Dieses Geschenk beinhaltete ein IT-Netzwerk mit Technik auch von Huawei und (in geringerem Maße) ZTE. Später stellte sich heraus, dass das Netzwerk jede Nacht große Datenpakete an ein Netzwerk in China übertrug, ohne dass die AU davon wusste oder dies wollte. In der Folge wurde die gesamte IT-Ausstattung der AU ausgetauscht, und nur vertrauenswürdige Lieferanten und Dienstleister durften daran teilnehmen.[116]

Im letzteren Fall hat China PNG über die Exim-Bank 53 Mio. US-Dollar geliehen, damit Huawei in PNGs Hauptstadt Port Moresby ein Datenzentrum als Teil des Integrated Government Information System (IGIS) bauen kann. Die Exim Bank ist mit der „Umsetzung von Pekings Handels- und strategischen Zielen" ("implementing Beijing's trade and strategic objectives") beauftragt.[117] Das Zentrum wurde gerade rechtzeitig für das Treffen der Staats- und Regierungschefs der Asiatisch-Pazifischen Kooperation (APEC) in Betrieb genommen. Das neu errichtete Rechenzentrum hatte zahlreiche und höchstwahrscheinlich absichtlich eingebaute gravierende Sicherheitslücken.[118] Diese wurden nur zufällig entdeckt, als PNG um finanzielle Unterstützung von Australien bat, um Mängel bei den Schutzmaßnahmen zu beheben. China finanzierte auch weitere digitale Infrastrukturprojekte in PNG, darunter den biometrischen Personalausweis und das nationale Breitbandnetz.[119]

Ein weiterer Fall, der wenig schmeichelhaftes Licht auf die Vertrauenswürdigkeit eines großen chinesischen Anbieters wirft, findet sich in den jüngsten Berichten über die diskriminierende und gezielte Erfassung ethnischer Minderheiten durch Gesichtserkennungssoftware, *"likely to cause further distrust of the company in the West"*[120] [121]

116 Sherman (2019).
117 The Australian Financial Review (2020).
118 The Australian Financial Review (2020).
119 ASPI (2020).
120 Endgadget (2020).
121 Washington Post (2020).

8 FAZIT UND SZENARIEN

Es ist schwierig, die wirtschaftlichen Kosten von nicht-vertrauenswürdigen Anbietern in 5G-Kommunikationsnetzen in Europa mit einem gewissen Grad an Genauigkeit zu schätzen. Ein Grund hierfür ist, dass die zukünftige Bedeutung dieser neuen Technologie für Wirtschaft und Gesellschaft schwer quantifizierbar ist und viele Fragen noch offen sind. Ein weiterer Grund sind die externen Kosten, die von anderen Marktteilnehmern als den Mobilfunknetzbetreibern getragen werden. Ein dritter Grund ist die zeitliche Verteilung der Kosten. Ein ganzheitlicher Abschätzungsansatz stünde daher von vornherein auf wackligen Beinen. Möglich jedoch ist die Erfassung von minimalen Größenordnungen in einigen Bereichen – also ein **additiver Schätzansatz,** der versucht, ein aus verschiedenen Gründen zu erwartendes Minimum an derzeit versteckten Kosten sichtbar zu machen.

Dieser additive Ansatz wird sich von Land zu Land unterscheiden, sowohl was den Inhalt - die Komponenten, die geschätzt werden können - als auch sein Ergebnis angeht, das auch von der Größe der jeweiligen Volkswirtschaft und ihrer Zusammensetzung abhängt. Aus diesem Grund werden wir uns einzelnen Ländern im Rahmen von Länderstudien zuwenden. Diese **Länderstudien** werden hoffentlich dazu beitragen, dass die Entscheidungsträger die Weichen für die Regulierung einer Infrastruktur und Technologie stellen, die für ein Jahrzehnt von unschätzbarer Bedeutung ist. Im **Anhang** zu diesem BIGS Standpunkt (Kap. 9) fassen wir die Ergebnisse der Länderstudien zusammen. Falls man für ein bestimmtes Land besonderes Interesse aufbringt, empfehlen wir, die vollständige Länderstudie zu lesen, die als separates Dokument verfügbar ist.

Die verschiedenen Kostenkategorien, die wir oben diskutiert haben, zeigen deutlich, dass eine Gesellschaft es nicht allein den Mobilfunknetzbetreibern überlassen kann, wen sie als Lieferanten für die zukünftige überkritische Infrastruktur auswählen. Während der Kauf von Produkten zu Dumpingpreisen aus individueller Unternehmensperspektive vorteilhaft sein mag (aber Vorsicht vor dem Lock-in-Effekt), ist er es sicher nicht für die Volkswirtschaft als Ganzes.

Das Versprechen von **OpenRAN** mit einer offeneren 5G-Netzarchitektur, die es den Mobilfunknetzbetreibern ermöglicht, aus einem größeren Spektrum von Anbietern zu wählen und die es ihnen auch erlauben würde, einzelne Komponenten ihres Netzes leichter auszutauschen, wird **die Marktmacht zugunsten der Betreiber verschieben**. Die Betreiber sollten daher diesen alternativen Ansatz zum Aufbau eines Netzes in Betracht ziehen und für sich selbst abwägen, ob es die mögliche Verzögerung bis zur Inbetriebnahme des 5G-Netzes wert ist. Allerdings wird der wirtschaftliche Effekt einer **Verzögerung der 5G-Verfügbarkeit** gelegentlich übertrieben. Da die „Killer-Applikationen" für 5G noch entwickelt werden, ebenso wie viele der 5G-kompatiblen Geräte, ist die neue Netzgeneration „nur" ein (viel) schnelleres Mobilfunknetz für schnelleren Internetzugang. Die großen Produktivitätsgewinne werden sich erst später einstellen.

Während viele der besprochenen Maßnahmen unabhängig von der Wahl des Anbieters umgesetzt werden müssen, macht der Grad des **Vertrauens in den Anbieter** als Unternehmen, aber auch der gesetzliche Rahmen, in dem ein Unternehmen agiert, einen großen Unterschied in der Höhe der Kosten. Wenn das Vertrauen in Zweifel gerät, wird der Grad an **Rechtsstaatlichkeit** zum nächstbesten Ersatz für Vertrauen. In dieser Hinsicht unterscheiden sich die fünf Systemanbieter erheblich. Zumindest zeigt die Erfahrung, dass eine Schadensersatzklage gegen ein Unternehmen in China weniger Aussicht auf Erfolg hat, als in Ländern mit hoher Rechtsstaatlichkeit.

Die Entscheidungsträger sollten aus mehreren verfügbaren und sich manchmal gegenseitig ausschließenden Alternativen eine Entscheidung treffen, die alle politischen, technischen, wirtschaftlichen und gesellschaftlichen Aspekte berücksichtigt. Diese Entscheidungen sind mit Unsicherheiten verbunden, da die Richtigkeit der Annahmen in einem schnelllebigen Umfeld in Frage gestellt werden kann. In diesem dynamischen Umfeld ist es für alle Marktteilnehmer (vielleicht mit Ausnahme der Anbieter) von großem Wert, Flexibilität zu haben oder zu gewinnen.

Eine Methode zur Unterstützung der Entscheidungsfindung in Situationen mit hoher Komplexität und Unsicherheit ist die Szenariotechnik. Die Szenariotechnik stammt aus dem Bereich der Wirtschaftswissenschaften und hat den Vorteil, dass drei konkrete Alternativen berechnet bzw. simuliert werden können. Mit dieser Technik können Annahmen über einzelne Werte systematisch angepasst und die Auswirkungen anschließend überprüft werden. Dadurch können Unsicherheiten bei der Entscheidungsfindung deutlich reduziert und die jeweiligen Optionen überprüft werden. Die einfachste Form der Szenarienbildung sieht drei Szenarien vor: optimistisch, realistisch und pessimistisch.

8.1 Optimistisches Szenario

China hält seine Versprechen. Huawei und ZTE werden nicht aufgefordert, unzulässige Absprachen mit der Kommunistischen Partei Chinas (KPCh) zu treffen. Sie könnten zwar per Gesetz dazu gezwungen werden, aber die KPCh ist eher am langfristigen Geschäftserfolg von Huawei und ZTE interessiert und wird diesen nicht gefährden, indem sie den Zugang nutzt, den sie durch diese Unternehmen zu westlichen 5G-Netzwerken erhalten könnte. Anders als bei allen traditionellen Cyberwerkzeugen, die von Chinas Geheimdiensten und verwandten Hackergruppen genutzt werden, werden die Möglichkeiten, die sich durch 5G ergeben, nicht genutzt werden (siehe Abschnitt Produktivitätskosten oben, speziell zu Opportunitätskosten).

Im Gegensatz zu früheren Erfahrungen in verschiedenen Branchen ist China der Meinung, dass es in Bereichen wie Industrie 4.0 und den Geschehen, die in westlichen Fabriken und F&E-Zentren vor sich gehen, bereits wettbewerbsfähig genug ist. Es wird die Möglichkeiten, die 5G bietet, nicht nutzen, um von der Chipindustrie zu lernen, die es im Moment so verzweifelt versucht zu kopieren (siehe Abschnitte Regulierungskosten, Versicherung, Verschiebung der Nachfrage, Veränderung des Angebots). Anders als bei der COVID-Impfstoffentwicklung wird China die Möglichkeiten, die sich aus 5G-kontrollierten Laboren und Experimenten ergeben, nicht ausnutzen.

Die EU und ihre Mitgliedstaaten können die Abhängigkeit von der 5G-Technologie aus China ignorieren, wenn sie über den Status Taiwans in internationalen Organisationen entscheiden oder wenn sie Sanktionen gegen China wegen Verstößen gegen das Völkerrecht, das Seerecht und Menschenrechtsverletzungen erwägen. Lock-in-Effekte können von den chinesischen Anbietern nicht ausgenutzt werden, da sich mit der weit verbreiteten Einführung von OpenRAN die Marktmacht zu Gunsten der Mobilfunknetzbetreiber verschoben hat.

Es ist daher eine Verschwendung von Geld und Ressourcen, wenn Mobilfunknetzbetreiber nicht das günstigste Angebot von Anbietern annehmen, die ihnen beim Aufbau der Netzwerke helfen. Grundlegende Sicherheitskosten müssen ohnehin implementiert werden, um die Netze vor Cyberkriminellen und Spionage aus Drittländern zu schützen. Die außenpolitische Strategie, die als „Wandel durch Handel" bekannt ist, wird schließlich erfolgreich sein und China wird sich im nächsten Jahrzehnt zu einem Land mit stärkerer Rechtsstaatlichkeit und Respekt für Eigentumsrechte entwickeln.

Wir finden dieses Szenario äußerst optimistisch und glauben, dass das Prinzip Hoffnung keine Strategie ersetzt. Stattdessen kann man auf das Beste hoffen, sollte sich aber auf das Schlimmste vorbereiten.

8.2 Pessimistisches Szenario

Mobilfunknetzbetreiber wählen den günstigsten Anbieter, mit dem sie ihre 5G-Netze aufbauen. Huawei und ZTE gewinnen zusammen einen großen Marktanteil in Westeuropa für 5G-Technik. Die Netze funktionieren ordnungsgemäß und zuverlässig, daher wickelt ein großer Teil der Wirtschaft seine Wertschöpfungskette über diese 5G-Netze ab. Schließlich nutzen auch Regierungen mit ihren verschiedenen Einrichtungen die vielfältigen Möglichkeiten der Digitalisierung. Das gilt auch für das Militär und andere Sicherheitsorganisationen. Aufgrund der vertieften europäischen Integration verstärken Sicherheits- und Geheimdienstinstitutionen ihre Zusammenarbeit und Interoperabilität, insbesondere wenn es um neue Fähigkeiten geht, wobei letztere oft auf 5G-Technologie beruhen.

Foto © CribbVisuals/iStockphoto

Während die chinesische Regierung ihre Wirtschaft und den internationalen Einfluss weiter ausbaut, missachtet sie kontinuierlich grundlegende Menschenrechte im eigenen Land sowie in Ländern und Gebieten, die unter ihrem Einfluss stehen. Sie respektiert weder das Völkerrecht noch das Seerecht. Die EU wird für ihre Werte eintreten und ihre wirtschaftliche und politische Stärke nutzen, um China mit Wirtschaftssanktionen zur Einhaltung dieser internationalen Normen zu zwingen, indem sie immer mehr politischen Aktivisten aus China Asyl gewährt und die europäischen Marinen an Manövern zur Offenhaltung von Handelsrouten teilnehmen.

An diesem Punkt entscheidet die KPCh, dass sie den Europäern eine Lektion erteilen will. Plötzlich spielen die Netzwerke in Europa verrückt. Sie funktionieren nicht mehr richtig und Unternehmen erleben Kaskadeneffekte ausgehend von den 5G-Netzwerken in andere kritische Infrastrukturen. Weil der öffentliche und der größte Teil des privaten Verkehrs zum Stillstand kommt, kehren Krankenhäuser zu einem Papier- und Bleistiftmanagement zurück, was ihre Kapazität stark reduziert. Was folgt, ist eine langandauernde tiefe Rezession in den europäischen Volkswirtschaften

Der Aufbau von Behelfslösungen, die sich nicht auf die 5G-Technik stützen, dauert Wochen, aber um die Produktivität wieder auf das Vorkrisenniveau zu bringen, ist ein Neustart der 5G-Netze - diesmal ohne chinesische Technik - notwendig und braucht weitere Zeit. Während die EU und ihre Mitgliedsstaaten die innenpolitische Krise bewältigen, haben sie keine Energie für weitere internationale Konflikte. China wird die Situation nutzen, um seinen internationalen Einfluss weiter auszubauen. Die Kosten für die Gesellschaft werden daher, wie in Kapitel 5 beschrieben, enorm sein und denen ähneln, die wir derzeit durch pandemiebedingte Ausfälle erleben. Darüber hinaus gibt es keinen Streit darüber, was die wirtschaftlich rationale Wahl bei der Auswahl eines Anbieters für 5G-Netze gewesen wäre.

Wir halten dieses Szenario für unwahrscheinlich, aber möglich. Wir kommen zu diesem Schluss, weil eine solche großflächige Abschaltung von 5G fast wie die „nukleare Option" für die Cyberwelt ist. Und wie wir

aus der Geschichte wissen, sind Länder glücklicherweise zurückhaltend, von einer solch verheerenden Option Gebrauch zu machen. Aber die Analogie ist auch irreführend. Im Gegensatz zu kinetischen Waffen kann eine solche Cyberwaffe nur einmal eingesetzt werden. Einmal benutzt und einem Staat zugeordnet, werden die Länder die Technik rauswerfen, die als Eintrittspforte in ihre Netzwerke diente. Danach ist es unmöglich, sie erneut einzusetzen. Folglich hätte eine solche Aktion auch schwerwiegende Auswirkungen auf zukünftige Geschäftsmöglichkeiten des angreifenden Landes. Außerdem kann der Angreifer in diesem Szenario nicht sicher sein, dass der Angriff unbeantwortet bleibt, und wenn er beantwortet wird, bleibt er möglicherweise nicht auf die Cyberwelt beschränkt.

8.3 Realistisches Szenario

Das realistische Szenario beginnt genauso wie das Armageddon-Szenario. In diesem Fall macht China jedoch nicht von seiner potenziellen Option Gebrauch, die europäischen Volkswirtschaften fast vollständig lahmzulegen. Stattdessen nutzt es den verdeckten Zugriff auf die kritische Infrastruktur, um Wissen und Erkenntnisse über europäische Unternehmen, Forschungseinrichtungen, Regierungen und politische Akteure zu gewinnen. Sie tut dies so, dass die Taten nicht unbestreitbar zugeordnet werden können, um unterhalb der Schwelle zu bleiben, bei der die Opfer geeignet zurückschlagen und die verdächtige Technik abreißen und ersetzen. Das durch diese Operationen gewonnene Wissen wird China und chinesischen Unternehmen helfen, weltweit weiter an politischer Macht und Marktmacht zu gewinnen. Nationale und EU-Versuche, technologisch zu den USA und China aufzuschließen (oder ihren Wettbewerbsvorteil zu behalten), verlieren an Effektivität, da das geistige Eigentum nicht ausreichend geschützt werden kann. Ericsson und Nokia werden ihre derzeit noch starke Marktposition verlieren und in den 2030er Jahren bei 6G keine Rolle mehr spielen. Schweden und Finnland werden darüber frustriert Deutschland und Frankreich die Schuld geben und behaupten, dass dies nicht zugelassen worden wäre, wenn es sich zum Beispiel um Siemens und Alcatel gehandelt hätte.

Einige sicherheitssensible Unternehmen werden die 5G-Technik von Huawei und ZTE in ihren privaten Netzen ersetzen und vielleicht zu einem OpenRAN-System wechseln, in dem sie nur vertrauenswürdige Anbieter zulassen. Alternativ schalten sie 5G für die Teile des Unternehmens ab, die sie als die Kronjuwelen ihrer Wertschöpfungskette betrachten. Die europäischen Geheimdienste werden gestärkt aus dieser Sache hervorgehen, da sie mit ihren Vorhersagen richtig lagen: *Die weltpolitische Situation und die damit im Zusammenhang stehenden politischen wie wirtschaftlichen Ambitionen Chinas lassen eine weitere Intensivierung der Spionageaktivitäten wie auch der Einflussnahmeaktivitäten erwarten.*[122] Der Militär- und Sicherheitsapparat wird sein eigenes Netz mit europäischer RAN-Technik aufbauen. Da aber auch unter den EU-Staaten Lauschangriffe nicht unbekannt sind, wird dies eher national abgeschirmt erfolgen, was die Einheit der EU untergräbt.

Die Kosten in einem solchen Szenario werden größtenteils verborgen bleiben und alle Elemente enthalten, die wir in Kapitel 6 besprochen haben. Diese Kosten sind eindeutig höher als das, was durch niedrigere Preise von nicht-vertrauenswürdigen Anbietern gewonnen werden kann. Sobald dies für politische Entscheidungsträger und die Öffentlichkeit offensichtlich wird, werden Fehlentscheidungen kompensiert. Letztendlich ist es in diesem Szenario absehbar, dass Länder und Mobilfunknetzbetreiber irgendwann die vertrauensunwürdige Technik ersetzen müssen. Für diesen Fall kann man zusammenfassend sagen, dass letztlich doppelt für diese neue Technik bezahlt werden müsste.

Ceteris paribus halten wir dies für das wahrscheinlichste Szenario, angesichts dessen, was wir wissen und im Laufe dieser Studie gelernt haben. Es sei denn, die westeuropäischen Regierungen beschließen eine Regulierung, die den chinesischen Zugang zu 5G-Netzen effektiv einschränkt. Wir sind uns bewusst, dass eine solche Entscheidung Zweitrundeneffekte haben wird, wie z.B. Vergeltungsmaßnahmen von China, die politische Entscheidungsträger berücksichtigen müssen.

Während wir diese Studie zu Ende bringen, startet die EU-Kommission eine Initiative in diese Rich-

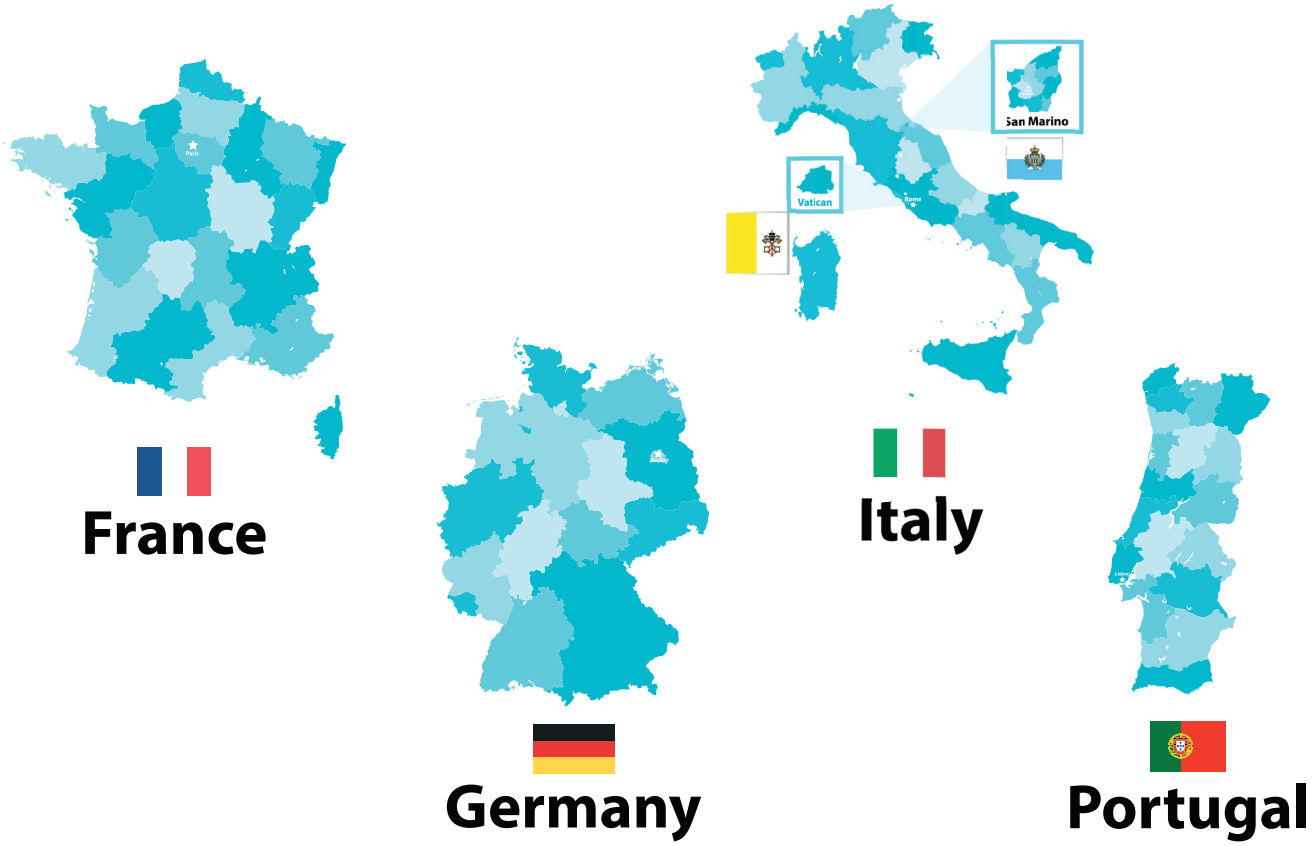
122 BfV 2019, S.298.

tung und fordert die Mitgliedsstaaten auf: "[to] (a) *ssess the risk profile of suppliers; as a consequence,* ***apply relevant restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks – for key assets*** *defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions)".*[123] Der Bericht weist zu Recht darauf hin, dass *"(p)rogress is urgently needed to mitigate the risk of dependency on high-risk suppliers, also with a view to reducing dependencies at Union level."*[124]

Viele Mitgliedsstaaten haben Maßnahmen ergriffen oder planen solche, um das Risiko, das von nicht-vertrauenswürdigen Anbietern ausgeht, zu begrenzen und damit die externen Kosten zu kompensieren, die deren Nutzung den europäischen Gesellschaften auferlegt. Es bleibt jedoch die Frage, ob diese Maßnahmen (falls sie umgesetzt werden) ausreichend sind.

Wir unterstützen die Maßnahmen der Kommission zur Stärkung der Forschung für die 6G-Entwicklung als Teil des Forschungsrahmenprogramms Horizont Europe von ganzem Herzen.[125] Wir glauben jedoch, dass ein dediziertes **Testzentrum für 5G-Sicherheit** benötigt wird und ein lohnenswertes EU-Vorhaben wäre. Wir hoffen, dass wir durch die Aufdeckung der versteckten Kosten von nicht-vertrauenswürdigen Anbietern in 5G-Netzwerken einen Beitrag zur Debatte der Forschungsgemeinschaft, aber auch und vor allem zur politischen Debatte darüber geleistet haben, wie der Aufbau und Betrieb der nächsten Generation kritischer Infrastrukturen angemessen reguliert werden kann.

123 EU Commission (2020), S.7, Hervorhebung durch die Autoren.
124 EU Commission (2020), S. 9.
125 EU Commission (2020), S. 12f.



Grafik © Oleg Chepurin /iStockphoto

9 ANHANG: SYNTHESE DER LÄNDERSTUDIEN FÜR FRANKREICH, DEUTSCHLAND, ITALIEN UND PORTUGAL

9.1 Einleitung

In den vorherigen Kapiteln haben wir gezeigt, wie welche Kosten durch nicht-vertrauenswürdige Technik in 5G-Netzen entstehen und wie diese ggf. ermittelt werden können. Auf dieser Grundlage haben wir Länderstudien für Deutschland, Frankreich, Italien und Portugal erstellt und einzelne Kostenkategorien berechnet. In diesem Anhang fassen wir die Länderstudien kurz zusammen und stellen die wichtigsten Ergebnisse vor.

Die hier beschriebenen Kosten sind nur eine **Auswahl der Kosten**, die nicht-vertrauenswürdige Anbieter für die finanziellen, wirtschaftlichen und politischen „Bilanzen" von Mobilfunknetzbetreibern, Kunden und Steuerzahlern bedeuten könnten, wie die Zuordnungstabelle der Kostenkategorien in der Zusammenfassung deutlich macht.

Nationale Volkswirtschaften, Telekommunikationsmärkte und regulatorische Fortschritte haben natürlich einen großen Einfluss auf die Höhe der Kosten, daher beschreibt dieses Kapitel zunächst kurz die 5G-Landschaft und den rechtlichen Kontext in den betrachteten Ländern.

9.2 Die 5G-Landschaft in Deutschland, Frankreich, Italien und Portugal

9.2.1 Deutschland

Für deutsche Stakeholder besteht ein mäßiges Risiko, dass versteckte Kosten von nicht-vertrauenswürdigen 5G-Anbietern entstehen, wenn die Maßnahmen im Entwurf für das IT-Sicherheitsgesetz 2.0 konsequent umgesetzt werden. Ansonsten besteht ein erhebliches Risiko für die deutsche Volkswirtschaft.

Die Entwicklung von 5G-Netzen in Deutschland liegt in den Händen von weitgehend bekannten Mobilfunknetzbetreibern, wird aber einen anderen Anbieter-Mix als bei 3G und 4G-Netzen beinhalten. Es gibt drei bestehende Mobilfunknetzbetreiber: Vodafone, Telefónica Deutschland und die Deutsche Telekom. Ein neuer, vierter Mobilfunknetzbetreiber, 1&1 (Drillisch), wird seine Rolle von einem Mieter der Netzwerkbandbreite anderer zu einem eigenständigen Betreiber weiterentwickeln. Obwohl die bestehenden Mobilfunknetzbetreiber alle nicht-vertrauenswürdige Hersteller-Hardware in ihrer 4G-Infrastruktur haben, plant scheinbar keines der vier Unternehmen mehr, chinesische 5G-Netzwerkausrüster in ihren 5G-Kernnetzen in Zukunft zu verwenden. Vodafone und die Deutsche Telekom wollen möglicherweise Huawei in ihren RAN-Netz verwenden, während 1&1 einen OpenRAN-Ausbau plant. Auch Telefónica scheint in diese Richtung zu tendieren.

Die deutsche Regierung hat bereits 2016 eine Strategie für 5G skizziert, mit dem Ziel, ein führender Markt für 5G-Anwendungen zu werden. Parallel zur Politik hat das Parlament 2015 eine wirksame Gesetzgebung zur Gewährleistung der IT-Sicherheit in Deutschland entwickelt. Mit dem Zweiten IT-Sicherheitsgesetz (IT-SiG 2.0), das sich Ende 2020 im Entwurfsstadium befindet, wird ein doppeltes Prüfverfahren für chinesische Systeme eingeführt. Dieses verlangt von den Herstellern die Unterzeichnung von Garantieerklärungen und unterzieht die Angebote einer Prüfung durch fünf kooperierende Ministerien und Behörden, die die Vertrauenswürdigkeit der Hersteller anhand von fünf verschiedenen Kriterien sicherstellen soll. Mit diesem strengen Regime wird es als nahezu sicher angesehen, dass nicht-vertrauenswürdige Hersteller in Zukunft von deutschen Netzen ausgeschlossen werden. Gleichwohl ist es kein vollständiger Bann nicht-vertrauenswürdiger Technik.

Die Entwicklung dieser Gesetzgebung spiegelt die nahezu universelle Skepsis gegenüber chinesischen Anbietern wider, wobei die meisten im Bundestag vertretenen Parteien Positionen vertreten, die von einer Regulierung zur Sicherstellung der Vertrauenswürdigkeit bis hin zum völligen Ausschluss reichen. Allerdings ist die regierende CDU/CSU in dieser Frage intern gespalten, was den Entscheidungsprozess innerhalb der Regierung erschwert.

9.2.2 Frankreich

Französische Stakeholder haben ein geringes Risiko, versteckte Kosten von nicht-vertrauenswürdigen 5G-Anbietern zu tragen.

In Frankreich gibt es vier Mobilfunknetzbetreiber, die bei der Einführung von 5G-Infrastrukturen führend sind - Orange, SFR, Bouygues und FREE. Orange hat gegenwärtig den größten Marktanteil. Im September 2020 haben diese Unternehmen Lizenzen für das Spektrum erworben, um 5G-Dienste für die nächsten 15 Jahre anzubieten. Jeder Mobilfunknetzbetreiber muss bis 2025 10.500 Antennen aufstellen, um das Ziel der französischen Regierung zu unterstützen, bis 2030 ein vollständiges 5G-Netz aufzubauen. Der 5G-Ausbau begann im November 2020 mit dem Einschalten einer Antenne in Nizza und wird voraussichtlich Stadt für Stadt abgeschlossen werden. In der nahen Zukunft wird sich der Ausbau nur auf das 5G-RAN konzentrieren. Das Kernnetz wird zunächst auf der 4G-Technik bleiben. Nur zwei von vier Anbietern nutzen die 4G-Ausrüstung von Huawei; am französischen 4G-Ausrüstungsmarkt hat Huawei nur einen Anteil von 20 %, und sein Anteil an der 5G-Ausrüstung wird voraussichtlich auf einem niedrigeren Niveau liegen (in einem Bereich von 15 bis 20 %).

Bedenken über nicht-vertrauenswürdige Anbieter wurden quer durch die Zivilgesellschaft, die Regierung und das politische Spektrum geäußert. Der französische Telekommunikationsmarkt ist bereits gut reguliert; drei Institutionen[126] spielen eine Schlüsselrolle bei

126 Die Nationale Agentur für Cybersicherheit Frankreichs (ANSSI), die Behörde für elektronische Kommunikation und Postregulierung (ARCEP) und die Nationale Agentur für Frequenzen (ANFR).

der Abwägung zwischen den ehrgeizigen Ausbauplänen der Regierung und den Bedenken hinsichtlich Cybersicherheit und Wettbewerb. In den Jahren 2019 und 2020 wurden zusätzliche Artikel in das französische Gesetzbuch für Post und elektronische Kommunikation aufgenommen, um sicherzustellen, dass Sicherheitsbedenken berücksichtigt werden. Nun müssen Mobilfunknetzbetreiber Anträge bei der französischen Cybersecurity-Agentur (ANSSI) einreichen. Von den bisher 157 Anträgen betrafen die 75 abgelehnten Anträge bzw. „Genehmigungen mit verkürzter Laufzeit" chinesische Geräte. Der französische Staat wird derzeit gerichtlich angefochten, weil er von Bouygues verlangt, 3.000 Huawei-Antennen und -Basisstationen in städtischen Gebieten bis 2028 zu entfernen.

9.2.3 Italien

Für italienische Stakeholder besteht nach wie vor ein geringes bis mäßiges Risiko, dass versteckte Kosten von nicht-vertrauenswürdigen 5G-Anbietern anfallen.

Die drei großen italienischen Mobilfunknetzbetreiber, TIM, Vodafone und WINDTRE, haben mit der Einführung von 5G-Diensten für Geschäfts- und Privatkunden in den größten italienischen Städten begonnen. Zwei kleinere Mobilfunknetzbetreiber, Iliad und Fastweb, streben die Einführung von Diensten Anfang 2021 an. Italien ist eines der vielen EU-Länder mit einer 4G-Infrastruktur, bei der mehr als 50 % der Komponenten von nicht-vertrauenswürdigen Anbietern stammen. Besonders niedrige Gewinnmargen im italienischen Telekommunikationsmarkt treiben die Mobilfunknetzbetreiber dazu, die Infrastruktur durch Partnerschaften gemeinsam zu nutzen (z.B. Türme und Backhauling) und sich für ein herstellerübergreifendes 5G-RAN zu entscheiden, wenn bereits Geräte auch von nicht-vertrauenswürdigen Anbietern installiert wurden. Allerdings können die Kosten für ein späteres Rip-and-Replace - zumindest von sensiblen „Kern"-Netzkomponenten - prohibitiv sein (d. h. Ausrüstung von nicht-vertrauenswürdigen Anbietern im Kern ist für die italienischen Mobilfunknetzbetreiber keine wirkliche Option).

Die italienische Regierung hat Ambitionen, das erste vollständig realisierte 5G-Netz unter den größeren europäischen Ländern zu sein. Italien war das erste EU-Land, das 5G-Spektrum an Mobilfunknetzbetreiber versteigerte, was am 2. Oktober 2018 abgeschlossen wurde. Italiens ungewöhnliche Struktur des Telekommunikationsmarktes – „Wholesale" – kann dazu beitragen, zukünftige versteckte Kosten zu reduzieren, indem die Kontrolle und Aufsicht über die Zugangs- und Transportkommunikation (Backhaul) bei einem Akteur zentralisiert wird, dessen Identifizierung jedoch noch nicht abgeschlossen ist.[127]

Italiens gesetzlicher Rahmen für die Einführung und Verwaltung einer sicheren 5G-Infrastruktur ist noch nicht vollständig fertiggestellt. Italien wendet die EU-Toolbox und seinen eigenen sogenannten Golden-Power-Rahmen an, wobei letzterer auf die 5G-Netze und -Betreiber ausgeweitet wurde.[128]

Zusätzlich müssen italienische Mobilfunknetzbetreiber Pläne für den Nationalen Cybersecurity Perimeter (NCP) einhalten und sie müssen die Prozesse, Technologien und Software in einem Nationalen Evaluierungs- und Zertifizierungszentrum (Centro di Valutazione e Certificazione Nazionale) testen. Die Rahmenbedingungen können streng und kostspielig sein, da jeder Mobilfunknetzbetreiber ein eigenes Network Operating Center benötigt und der NCP die Einrichtung eines Nationalen Bewertungs- und Zertifizierungszentrums im Jahr 2021 vorschreibt, bei dem die Betreiber ihre Pläne einreichen müssen.

2019 empfahl der italienische Parlamentsausschuss für die Sicherheit der Republik (COPASIR) der italienischen Regierung in seinem unveröffentlichten Bericht, Huawei von italienischen 5G-Netzen auszuschließen. Die Regierung hat bislang jedoch keine endgültige Entscheidung getroffen. Mit der Entwicklung des NCP hat die Regierung nun jedoch ein Dekret verabschiedet, das es nicht-vertrauenswürdigen Anbietern erlaubt, 5G-Infrastrukturen zu entwickeln, solange sie sich an festgelegte Regeln halten.

127 Theoretisch wird dieser zentrale Akteur OpenFiber sein, der den Großteil des ländlichen und derzeit wenig bekannten Glasfasernetzes gebaut hat (ein separates Glasfasernetz existiert auch im Besitz von TIM und Fastweb). Ein weiterer Akteur ist die Turmgesellschaft INWIT (Infrastrutture Wireless Italiane), die als privates Unternehmen aus der Fusion von TIM- und Vodafone-Assets entstanden ist. INWIT beherbergt nicht nur Betreiber auf seinen Türmen, sondern baut auch eigene DAS-Infrastrukturen (Distributed Antenna System), um eine weitreichende Abdeckung von dicht frequentierten Freiflächen oder großen geschlossenen Räumen zu ermöglichen, die für kommerzielle Aktivitäten, Freizeit und Sport (Stadien) oder Gesundheitsinfrastruktur (Krankenhäuser) vorgesehen sind. Das Wholesale-Modell und seine Führung steht heute im Mittelpunkt der politischen Diskussion, wobei sowohl technische als auch geschäftliche Fragen auf dem Tisch liegen.

128 Die italienische Regierung hat das Recht, die „goldene Macht" (vergleichbar mit „golden share") auszuüben, indem sie Übernahmen und Unternehmenstransaktionen von Unternehmen, die „strategische" Vermögens-werte in Italien besitzen, ablehnt oder konditioniert.

9.2.4 Portugal

Portugiesische Stakeholder gehen in einer dynamischen Umgebung ein mittleres bis hohes Risiko ein, versteckte Kosten von nicht-vertrauenswürdigen 5G-Anbietern zu tragen.

Die portugiesische Regierung hat ehrgeizige Pläne, um einen florierenden 5G-Sektor im Land zu fördern. Ursprünglich war geplant, 90 % der Bevölkerung bis 2025 zu versorgen. Der Fortschritt und die Steuerung dieses Prozesses wurden jedoch durch rechtliche Anfechtungen etablierter Mobilfunkbetreiber gegen die portugiesische Regulierungsbehörde ANACOM verzögert. Eine geplante Versteigerung von Frequenzen im Wert von 237,9 Mio. Euro und die Installation von Geräten durch nicht-vertrauenswürdige Anbieter könnte noch außerhalb eines vereinbarten Rahmens stattfinden. Alle drei großen Mobilfunknetzbetreiber (NOS, Vodafone und Altice) und zwei kleinere Betreiber werden bei der bevorstehenden Auktion um den Erwerb von Frequenzblöcken mitbieten, neben neuen Marktteilnehmern und ausländischen Bietern, die als herausfordernde Bieter besondere Bedingungen genießen werden. Die drei größten Mobilfunknetzbetreiber haben erklärt, dass sie für ihre Kernnetzinfrastruktur nicht von vertrauensunwürdigen Anbietern kaufen werden, obwohl keine Verpflichtung in Bezug auf ihr RAN eingegangen wurde.

Der Ansatz Portugals weicht von dem der meisten westeuropäischen Staaten ab. Die portugiesische Regierung hat trotz des Drucks der Europäischen Kommission keine Gesetze erlassen, um die Risiken, die von nicht-vertrauenswürdigen Anbietern ausgehen, zu managen oder diese auszuschließen. Der Ansatz der Regierung scheint ein Risikomanagement durch Gerätezertifizierung und -zulassung zu sein. Am 7. Februar 2020 beauftragte die Regierung jedoch die Einrichtung einer Task Force innerhalb des Hohen Rates für die Sicherheit des Cyberraums (CSSC), um die Umsetzung zukünftiger Regulierungsinstrumente sicherzustellen, eine Roadmap für die Cybersicherheit im Zusammenhang mit 5G-Netzwerken zu entwickeln und als leitender Monitor für Risiko und Risikomanagement zu fungieren.

9.2.5 Zusammenfassung

Nicht-vertrauenswürdige Anbieter werden wahrscheinlich weiterhin in hybriden 4G/5G-Kernnetzen und 5G-RANs zum Einsatz kommen, da es keine Vorschriften gibt, die bestehende 4G-Infrastruktur zu ersetzen und den Einsatz von nicht-vertrauenswürdigen Anbietern in 5G-Netzen einzuschränken. Viele Netzbetreiber sind aber noch in der Planung ihrer 5G-Netze und so stellt die nachfolgende Darstellung nur unseren gegenwärtigen Wissensstand dar.

Tabelle 9: Wahrscheinliche zukünftige Präsenz von nicht-vertrauenswürdigen Anbietern in 5G-Infrastrukturen

	Präsenz nicht-vertrauenswürdiger Anbieter in 5G-Infrastrukturen			
	Mobilfunknetzbetreiber	**4G**	**5G Kern**	**5G RAN**
Deutschland	Deutsche Telekom Vodafone Deutschland Telefónica Deutschland 1&1 Drillisch Netz	Ja Ja Ja X	Nein Nein Nein Unbekannt	Erwartet Erwartet ORAN ORAN
Frankreich	Orange France Free Telecom France Bouygues Telecom France SFR France	Nein Nein Ja Ja	Nein Nein Nein Nein	Nein Nein Ja Ja
Italien	WINDTRE Vodafone TIM Fastweb Iliad	Ja Ja Ja Ja Nein	Nein Nein Nein Nein Nein	Ja Ja Nein Nein Nein
Portugal	Vodafone Altice NOS	Ja Ja Ja	Nein Nein Nein	TBD Erwartet Erwartet

Quelle: eigene Darstellung.

9.3 Veränderung der Angebotsseite: die Kosten für das Verbot von nicht-vertrauenswürdigen Anbietern

Die Kosten für das Verbot nicht-vertrauenswürdiger Anbieter für Mobilfunknetzbetreiber und Volkswirtschaften sind nicht unerheblich, verblassen aber im Vergleich zum Ausmaß der zukünftigen offensichtlichen und versteckten Kosten von nicht-vertrauenswürdigen 5G-Netzen.

Die Abhängigkeit von herstellerspezifischen, nicht-vertrauenswürdigen Anbieterprodukten in bestehenden Telekommunikationsnetzen macht es für Mobilfunknetzbetreiber finanziell attraktiv, zumindest vorläufig mit diesen Anbietern an 5G zu arbeiten. Das Verbot von nicht-vertrauenswürdigen Anbietern in einem Land wird die Mobilfunknetzbetreiber voraussichtlich mehr Geld kosten, um in die teurere Infrastruktur vertrauenswürdiger Anbieter zu investieren, als im Basisszenario, und könnte zu Verzögerungen bei der Einführung von 5G-Diensten führen.

Wie wir in Kapitel 6 gesehen haben, gibt es zwei große quantifizierbare Kostenauswirkungen eines Verbots. Dabei handelt es sich erstens um den „Preiseffekt" – erhöhte Kosten für die Mobilfunkbetreiber, die auf die Rechnungen der Kunden umgelegt werden – und zweitens um den „Wachstums-/Wohlfahrtseffekt" – die Kosten, die dadurch entstehen, dass die Kunden Produktivitätsvorteile verlieren, einhergehend mit einem geringeren Wachstum des BIP, weil sie auf den Zugang zu 5G warten. Eine originäre Untersuchung dieser Kosten würde den Rahmen dieser Studie sprengen, daher stützen wir uns teilweise auf die von Huawei in Auftrag gegebene Studie 'Restricting Competition in 5G network equipment throughout Europe'[129] von Oxford Economics und ihr zentrales Szenario als Grundlage. Wir halten jedoch einige der zugrundeliegenden Annahmen dieser Studie für unrealistisch und die Schlussfolgerungen für überzogen. Generell gehen wir von folgenden Annahmen aus:

1. Der Wettbewerb bei den Ausstattungspreisen dürfte hart bleiben, auch wenn die Anzahl der Systemanbieter von 5G-Netztechnik reduziert wird;

2. die Verfügbarkeit von OpenRAN reduziert die Abhängigkeit der Mobilfunknetzbetreiber von einzelnen Anbietern und erhöht ihre Verhandlungsmacht, was sich auf die Preise auswirkt;[130]

3. die Umsätze der europäischen Mobilfunknetzbetreiber könnten höher ausfallen als erwartet[131], und die Mobilfunknetzbetreiber könnten die Preise für die Verbraucher moderater erhöhen;[132]

4. Faktoren wie COVID-19, Rechtsstreitigkeiten, regulatorische Verzögerungen, Politik, scheinen weitaus größere Verzögerungen bei der 5G-Einführung zu verursachen als die Zeit, die für den Wechsel zu vertrauenswürdigen Anbietern benötigt wird;[133]

5. Verzögerungen spielen möglicherweise kaum eine Rolle – die Nachfrage nach Machine-to-Machine-Anwendungen, die den größten Anteil der 5G-bedingten BIP-Zuwächse ausmachen werden, wird wahrscheinlich erst Mitte der 2020er Jahre steigen.[134]

In Anbetracht dieser Punkte:

- In **Deutschland** beschreibt das „zentrale Szenario" des Oxford Economics Reports **erhöhte Kosten** von rund **479 Mio. Euro** pro Jahr für Mobilfunknetzbetreiber, um 5G-Netze mit vertrauenswürdigen Anbietern aufzubauen. Das bedeutet, wenn man es auf die aktuelle Anzahl der bestehenden Mobilfunkverträge herunterbricht, nicht mehr als **3,18 Euro pro Vertrag**.[135] Oxford Economics errechnet außerdem einen BIP-Verlust von rund **6,9 Mrd. Euro** – oder **83 Euro pro Kopf**[136] – bis 2035.

129 Oxford Economics (2020).
130 BIGS Länderstudie Deutschland.
131 Ericsson (2019).
132 Wagener (2020).
133 Bestätigt durch Interviews mit Leitern von Mobilfunknetzbetreibern, die für die detaillierten Länderstudien hinter diesem Kapitel durchgeführt wurden.
134 Bestätigt durch Interviews mit Leitern von Mobilfunknetzbetreibern, die für die detaillierten Länderstudien hinter diesem Kapitel durchgeführt wurden.
135 Wir teilen den Preiseffekt durch die Anzahl der SIM-Karten innerhalb der Volkswirtschaft. Deutschland hatte im Jahr 2020 rund 150 Mio. aktive SIM-Karten.
136 Basierend auf der Bevölkerung 2019 von 83,02 Mio. Menschen.

Foto © sdecoret/iStockphoto

- **Frankreich**, ein kleinerer Telekommunikationsmarkt, sieht sich einem ähnlichen **Preiseffekt von 447 Mio. Euro** pro Jahr oder etwa **5,81 Euro pro Telefonvertrag gegenüber.**[137] Dies ist überraschend, wenn man bedenkt, dass Huawei nur etwas weniger als 20 % des Infrastrukturmarktes in Frankreich haben wird. Laut Oxford Economics droht Frankreich ein größerer potenzieller BIP-Verlust als Deutschland, nämlich **7,3 Mrd. Euro** bis 2035 oder **106,09 Euro pro Kopf.**[138] Allerdings sehen die französischen Telekom-Chefs auch nur geringe Auswirkungen auf die Produktivität, wenn sich der 5G-Ausbau um zwei bis drei Jahre verzögert.[139]

- In **Italien** müssen Kunden laut Oxford Economics mit einem Preiseffekt von rund **282 Mio. Euro** pro Jahr rechnen, was wiederum nicht mehr als **2,74** Euro pro Vertrag entspricht.[140] Die befragten italienischen Mobilfunknetzbetreiber haben jedoch erklärt, dass der Wechsel zu europäischen 5G-Anbietern billiger sein wird als für 2019 erwartet und ihre Marktanteile nicht durch den Ausschluss von nicht-vertrauenswürdigen Anbietern beeinträchtigt werden.[141] Ein Ericsson-Bericht schätzt, dass die Mobilfunknetzbetreiber auch ihre Umsätze bis 2030 steigern werden. Dem Land könnte bis 2035 ein BIP-Verlust von rund **4,7 Mrd. Euro** drohen, was wir als **77,87 Euro** pro Kopf berechnen.[142]

- Zuletzt **Portugal** – der kleinste Markt und am wenigsten fortgeschritten bei 5G - sieht sich einem **Preiseffekt von rund 63 Mio. Euro** gegenüber, oder **5,29 Euro pro Telefonvertrag**.[143] Über **500 Mio. Euro** könnten bis 2035 dauerhaft vom BIP abgezogen werden, das sind **8,28 Euro pro Kopf.**[144] Da die Bevölkerung jedoch so stark auf wenige Bezirke konzentriert ist, wird der Ausbau schnell große Teile der Bevölkerung erreichen, was

137 Frankreich hatte im Jahr 2020 rund 96,2 Mio. aktive SIM-Karten, einschließlich M2M-Anwendungen.
138 Basierend auf der Bevölkerung 2019 von 68,8 Mio. Menschen.
139 Öffentliche Aussagen und Interviews von SystemX.
140 Italien hatte im Jahr 2020 rund 103,7 Mio. aktive SIM-Karten.
141 Italienische Länderstudie von CEFRIEL.
142 Basierend auf der Bevölkerung 2019 von 60,36 Mio. Menschen.
143 In Portugal waren im Jahr 2020 rund 17,1 Mio. aktive SIM-Karten im Umlauf.
144 Basierend auf der Bevölkerung 2019 von 10,29 Mio. Menschen.

bedeutet, dass die BIP-Verlustprognosen nicht als linear angesehen werden sollten.[145] Regierungsbedingte Verzögerungen bei der Versteigerung des 5G-Spektrums und der Regulierung sind mit ziemlicher Sicherheit das systemische Problem und nicht die Verlagerung zu neuen Anbietern.

Selbst wenn es europäischen Mobilfunknetzbetreibern erlaubt wäre, nicht-vertrauenswürdige Produkte zu installieren, **ist es unwahrscheinlich, dass die Zusammenarbeit mit solchen Anbietern auf lange Sicht finanziell attraktiv bleibt.** Das „Dumping" billiger Produkte durch diese Firmen könnte Teil einer Strategie sein, um Nokia und Ericsson zum Ausstieg aus dem 5G-Markt zu zwingen, den Wettbewerb einzuschränken und die Aussicht zu erhöhen, dass Mobilfunknetzbetreiber mit nicht-vertrauenswürdigen Anbietern zusammenarbeiten und dann in Zukunft die Preise erhöhen können. Langfristig gesehen werden die Mobilfunknetzbetreiber in Zukunft auch auf 6G aufrüsten müssen, während chinesische Firmen wenig Anreiz haben werden, die Preise niedrig zu halten. Dies ist wahrscheinlich die bevorzugte Situation für chinesische Firmen, was sich darin zeigt, dass sie wenig Interesse an der Integration von OpenRAN-Standards zeigen (die es ermöglichen, dass Geräte verschiedener Hersteller in einem 5G-Netzwerk zusammenarbeiten).

9.4 Offensichtliche Kosten von nicht-vertrauenswürdigen Anbietern nach Land

Kompromittierte 5G-Netze könnten Volkswirtschaften im Falle zwischenstaatlicher Spannungen oder eines Konflikts mit China Dutzende von Milliarden Euro kosten.

Bevor wir uns den versteckten Kosten zuwenden, ist es sinnvoll, die offensichtlichen Kosten zu betrachten, die dadurch entstehen, dass nationale Netze übermäßig anfällig für Angriffe und Einmischungen durch ausländische Mächte sind. Wie in Kapitel 5 beschrieben, ist es schwierig, die offensichtlichen Kosten, die unter „normalen" Szenarien entstehen, zu bewerten.[146] Es ist jedoch möglich, die offensichtlichen Kosten, die bei schweren geopolitischen Spannungen auftreten können, auf zwei Arten zu untersuchen.

Ein **erster Ansatz** ist die Betrachtung der finanziellen Auswirkungen eines mehrtägigen Totalausfalls des Netzes – und des **Stillstands der Wirtschaft** – auf das BIP. Mit diesem Referenzrahmen könnte Deutschland als Europas größte Volkswirtschaft mit einem BIP von ca. 3,5 Mrd. Euro mit erheblichen Kosten konfrontiert werden[147]. Bei einem verlorenen Arbeitstag in Höhe von ca. 4,31 Mrd. kostet ein **3-tägiger Stillstand** demnach ca. **12,94 Mrd. Euro** und ein **6-tägiger Stillstand 25,88 Mrd. Euro**, also fast 0,75 % des BIP. Es scheint unvorstellbar, dass die Netzdienste innerhalb weniger Tage vollständig wiederhergestellt werden können, da das Ausmaß der erforderlichen Aufräumarbeiten in ganz Deutschland enorm wäre.

Ein **zweiter Ansatz** besteht darin, die **„Größenordnung" der Kosten verschiedener Ereignisse** (Fälle) anhand einer logarithmischen Skala zu betrachten. Eine solche Skala für die Messung von Vorurteilen hilft, vier Szenarien – siehe unten – nach ihrem Schweregrad besser zu differenzieren und die sehr wichtigen Unterschiede zwischen ihnen besser zu zeigen.

Fall A – Eine vollständige und endgültige Blockade von 100 % der Telekommunikationsinfrastruktur eines Mobilfunknetzbetreibers, die einen Blackout von privaten und geschäftlichen Telefongesprächen, SMS, MMS und mobilen Internetdiensten verursacht.

145 Mit dem Ausbau in den Regionen Lissabon und Porto erreicht 5G schnell rund 50 % der Bevölkerung.

146 Die materiellen und immateriellen Auswirkungen von subtilen Angriffen, die darauf abzielen, Daten zu stehlen oder zu manipulieren, die Auswirkungen von „Slow Burn"-Spionage und die langfristige Verlangsamung - „Drosselung" - von Netzwerken durch einen Gegner sind extrem komplex zu kalkulieren. Eine länderübergreifende Betrachtung ist sogar noch schwieriger, da die Ausgangsannahmen komplex und konstruiert sind, um einen Vergleich zu ermöglichen.

147 Statistisches Bundesamt (2020).

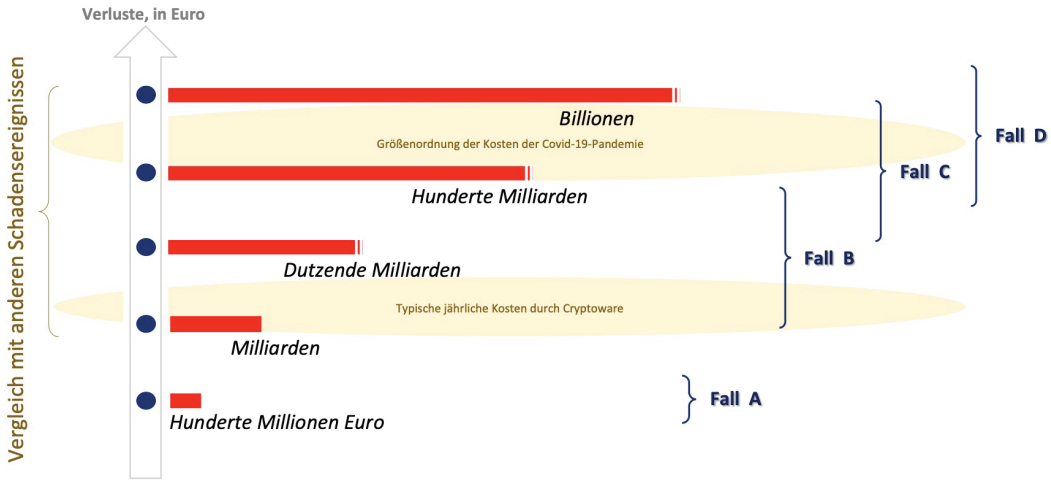
Fall B – Die Blockade betrifft auch das Internet der Dinge, industrielle Anwendungen (Fabrik 4.0), oder kommunizierende Fahrzeuge.

Fall C – Zusätzlich zu A und B erfolgt ein Angriff auf Daten, Programme und Software (im Besitz von Personen, Unternehmen, Verbänden, Verwaltungen) über die von einem Anbieter bereitgestellte 5G-Infrastruktur, was zu deren endgültiger Zerstörung, Verschlüsselung oder Unzugänglichkeit führt.

Fall D – Zusätzlich zu Fall C gibt es auch vorhergehende Fälschungen dieser Daten, Programme und Software, die Auto-, Zug- oder Schiffsunfälle, Haushaltsunfälle, medizinische und industrielle Katastrophen verursachen.

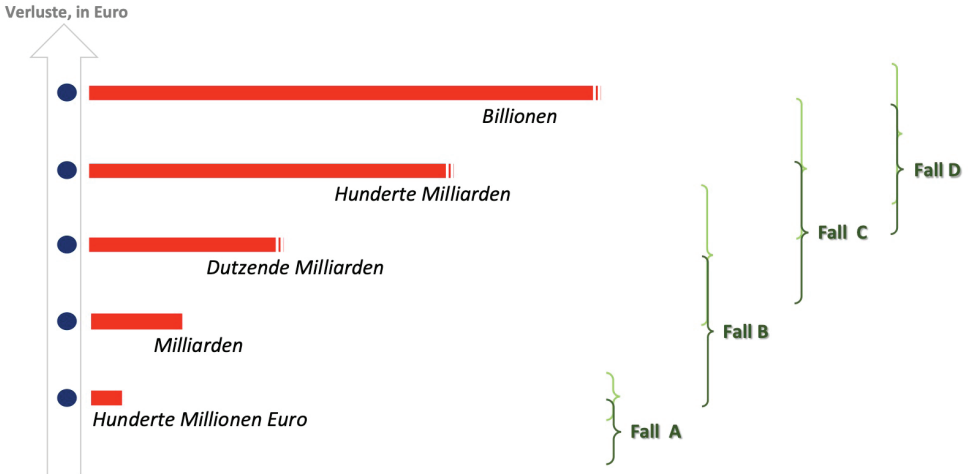
Die Methode wurde für Frankreich entwickelt, so dass andere Länder mit den Ergebnissen verglichen werden können. Als Volkswirtschaften von ähnlicher Größe werden Frankreich und Italien wahrscheinlich ähnliche Verluste bei jedem der Fälle erleiden:

Abbildung 4: Skalierung der Schäden für Frankreich und Italien (Euro)



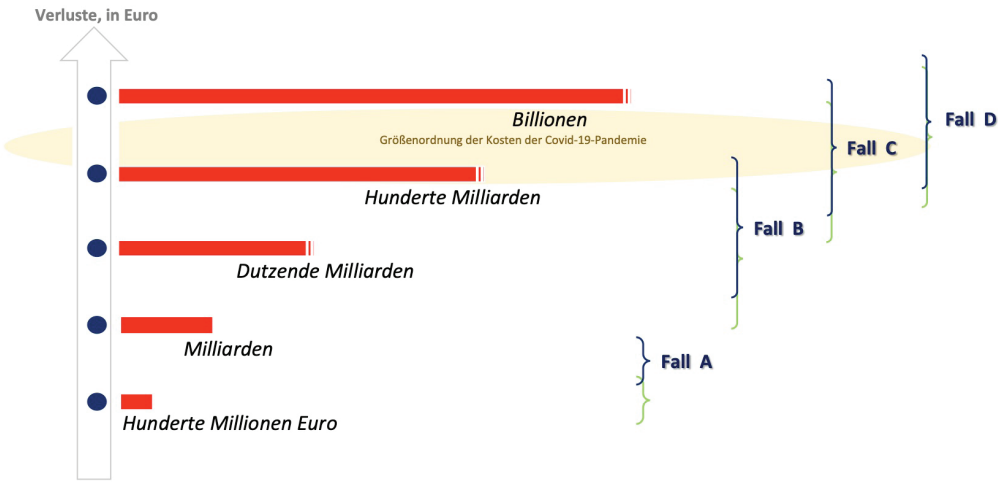
Als kleinste Volkswirtschaft dürfte Portugal in absoluten Zahlen am wenigsten leiden, aber relativ zu seiner Größe nicht unerheblich. (Frankreich: hellgrün)

Abbildung 5: Skalierung der Schäden für Portugal (Euro)



Als größte Volkswirtschaft, in der nicht-vertrauenswürdige Anbieter die größte Rolle spielen, hat Deutschland die höchsten Kosten zu erwarten. (Frankreich in hellgrün)

Abbildung 6: Skalierung der Schäden für Deutschland (Euro)



9.5 Die versteckten Kosten von nicht-vertrauenswürdigen 5G-Anbietern

Der Bericht skizziert nun die versteckten Kosten des Verbleibs bei nicht-vertrauenswürdigen Anbietern für Deutschland, Frankreich, Italien und Portugal, nachdem er die Kosten der Trennung von nicht-vertrauenswürdigen 5G-Anbietern und die offensichtlichen Kosten der Manipulation von nicht-vertrauenswürdigen Infrastrukturen während internationaler Unruhen oder Kriege behandelt hat.

9.5.1 Prüfzentren

Zentren für die Bewertung und Zertifizierung von 5G-Hardware, -Software und -Netzbetrieb würden die Steuerzahler der größten Volkswirtschaften fast 60 Mio. Euro pro Jahr kosten

Wie wir in Kapitel 6 argumentiert haben, sind selbst vertrauenswürdige 5G-Netzwerke anfällig für Angriffe und Subversion. Umsichtige Regierungen werden immer den Wunsch haben, Telekommunikationsinfrastrukturen und Lieferketten unabhängig zu zertifizieren, um Schwachstellen zu mindern. Da die Netzwerke und die Technologie mittlerweile so komplex sind, übersteigt die Zertifizierungsaufgabe zunehmend die Kapazitäten der Mobilfunkbetreiber. Nicht-vertrauenswürdige Anbieter erhöhen theoretisch die Kosten für diese Aktivitäten erheblich, da die Tests ohne die Kooperation des Anbieters durchgeführt werden müssen, was eine breitere und gründlichere Prüfung sowie die Entwicklung eines Prüfstands und digitaler „Zwillings"-Netzwerke erfordert, um zu verstehen, wie das reale Netzwerk missbraucht werden könnte.

Die genaue Kostenermittlung für staatliche Testzentren ist eine Herausforderung.[148] Die Gleichsetzung von Kosten, die für die vollständige Prüfung und Absicherung der Produkte von Anbietern ausgegeben werden, ist ebenfalls problematisch. Die Höhe der Kosten hängt von dem erforderlichen Grad der Prüfung und Simulation von Geräten und Netzwerkfunktionen ab. In absoluten Zahlen sind die (durch die nationale Gesetzgebung festgelegten) Zuständigkeiten, das Gehalt und die Kapitalkosten die wichtigsten Determinanten. Ein einfacher Ansatz besteht darin, die Kosten für ähnliche angewandte Forschungslabors

148 Wir können sowohl Top-Down-Kalkulationstechniken (mit Blick auf analoge Zentren) als auch Bottom-Up-Kalkulationstechniken (mit Schätzungen der Kosten von Prozessen wie Software-Reviews, Lieferketten-Audits und Netzwerküberwachungskosten nach Zeit) einsetzen.

als Benchmark für das jeweilige Land zu nehmen. Die Verteilung der Kosten hängt vom Grad der gemeinsamen Finanzierung zwischen Regierung und Mobilfunkbetreibern ab. In Großbritannien wird das unabhängige Huawei Cyber Security Evaluation Centre tatsächlich von Huawei finanziert, aber von einem Aufsichtsgremium verwaltet und kontrolliert, zu dem auch das National Cyber Security Centre der britischen Regierung gehört.

Wir schätzen, dass das nationale Testzentrum in Deutschland bis zu 60 Mio. Euro kosten könnte. Auf der Grundlage von Schätzungen der Marktgröße und des Umfangs der Rolle nicht-vertrauenswürdiger Anbieter in den jeweiligen Märkten könnte das französische Testzentrum bis zu 30 Mio. Euro kosten, hauptsächlich aufgrund der Personalkosten mit einem Bedarf von etwa 150 Experten und Verwaltungspersonal; das italienische 40 Mio. Euro und das portugiesische 20 Mio. Euro.

9.5.2 Kosten von Datenschutzverletzungen

Datenschutzverletzungen in größeren Volkswirtschaften, die in erheblichem Maße auf nicht-vertrauenswürdige Anbieterinfrastrukturen angewiesen sind, könnten Kosten in Milliardenhöhe verursachen.

Datenschutzverletzungen (Abschöpfen von Daten) sind eine Tatsache in Kommunikationsnetzwerken, insbesondere in solchen, die sich über ein ganzes Land erstrecken. Wenn wir Schätzungen für die „versteckten Kosten" von Datenschutzverletzungen in der 5G-Zukunft anbieten, schätzen wir tatsächlich die nationalen jährlichen Kosten für die prognostizierte Menge an Datenschutzverletzungen, die zu erwarten sind, während sich Daten im Transit über Netzwerke befinden, die von nicht-vertrauenswürdigen Anbietern betrieben werden. Wir stellen Vermutungen über potenzielle Wachstumsraten bei der Cyberkriminalität in Bezug auf Daten im Transit und Wachstumsraten bei den Kosten für Datenschutzverletzungen an und verwenden verfügbare Annahmen über die Durchdringung von 5G-Infrastrukturen in westeuropäischen Infrastrukturen (als Anteil des gesamten Datenübertragungsvolumens) und den Anteil, der voraussichtlich Infrastrukturen nicht vertrauenswürdiger Anbieter nutzen wird. Die Schätzungen sind wahrscheinlich zu niedrig angesetzt, da die Berücksichtigung des Wachstums der Maschine-zu-Maschine-Anforderungen an das Verkehrsvolumen extrem schwierig ist.

- In **Deutschland** belaufen sich nach unserem Modell die Kosten für Datenschutzverletzungen, die auf die Präsenz nicht-vertrauenswürdiger Anbieter in 5G-Netzen zurückzuführen sind, im Jahr 2024 auf bis zu **18 Mrd. Euro**, so die Beteiligung nicht-vertrauenswürdiger Netzwerkausrüster unreguliert bleibt. Ein großer Markt hat natürlich ein entsprechendes Kommunikationsvolumen, von dem wir erwarten, dass mehr als ein Viertel (29 %) bis 2024 über 5G-Netze laufen wird, und 50 % dieser 29 % könnten über nicht-vertrauenswürdige Netze geleitet werden, wenn das IT-Sicherheitsgesetz 2.0 nicht dazu führt, dass nicht-vertrauenswürdige Anbieter aus dem Netz herausgehalten werden.

- Für **Frankreich** schätzen wir Kosten in der Größenordnung von **623 Mio. Euro** für das Jahr 2024. Der Anteil des Datenverkehrs, der über nicht-vertrauenswürdige 5G-Netze abgewickelt wird, ist voraussichtlich geringer als in Deutschland und Portugal. So werden nicht-vertrauenswürdige Anbieter wahrscheinlich einen Marktanteil von weniger als 20 % haben und hauptsächlich ländliche Gebiete abdecken. Allerdings ist die Anzahl der gemeldeten Datenschutzverletzungen in Abb. 3 für Frankreich unrealistisch niedrig. Alternativ haben wir daher in einer zweiten Berechnung angenommen, dass die Anzahl der Datenschutzverletzungen mit der von Deutschland vergleichbar ist. In diesem Fall lägen die Kosten in der Größenordnung von **4,5 Mrd. Euro.**

- In **Italien** schätzen wir die jährlichen Kosten für Datenschutzverletzungen bis 2024 auf rund **580 Mio. Euro**. Dies ist zwar überraschend niedrig, aber der Grund dafür ist, dass Datenschutzverletzungen über nicht-vertrauenswürdige 5G-Trägernetzwerke wahrscheinlich einen geringen Anteil an den gesamten Datenschutzverletzungen in Italien ausmachen. Interviews mit Mobilfunknetzbetreibern und Analysen haben bestätigt, dass die Abhängigkeit der italienischen Betreiber von nicht-vertrauenswürdigen Anbietern wahrscheinlich gering sein wird - Huawei und ZTE werden bis 2024 nur 8,9 % der Gesamtkapazität bereitstellen. Außerdem ist die Anzahl der gemeldeten Datenschutzverletzungen in Italien unrealistisch niedrig

(siehe Abb. 3), und die durchschnittlichen Kosten einer Datenschutzverletzung sind im Vergleich zu Deutschland geringer. Nimmt man auch hier an, dass die Anzahl der Fälle proportional denen in Deutschland gleicht, so betragen die Kosten bereits 1,65 Mrd. Euro.

- In **Portugal**, dem kleinsten Markt, schätzen wir die jährlichen Kosten für Datenschutzverletzungen bis 2024 auf rund **133 Mio. Euro**.[149] Unter Verwendung offizieller Daten des Nationalen Zentrums für Cybersicherheit für die letzten 5 Jahre gehen wir davon aus, dass die Cyberkriminalität bei Daten im Transit für Portugal stärker zunehmen wird als im weltweiten Durchschnitt.[150] Wir schätzen jedoch auch, dass ein geringerer Teil des Datenverkehrs über Geräte nicht-vertrauenswürdiger Anbieter abgewickelt werden wird als in Deutschland (30 % im Vergleich zu 50 % +), da nicht-vertrauenswürdige Anbieter in der portugiesischen 4G-Infrastruktur oder den 5G-Infrastrukturplänen nicht so dominant sind.

Tabelle 10: Voraussichtlicher Anstieg der nationalen Kosten für Datenschutzverletzungen, die über ein nicht-vertrauenswürdiges 5G-Netzwerk auftreten

	Kosten in Millionen €		
	2022[151]	**2023**	**2024**
Deutschland	16.399,44	16.272,34	18.009,26
Frankreich	567,31	562,91	623,00
Frankreich[152]	4.142,77	4.110,66	4.549,43
Italien	528,28	524,48	580,46
Portugal	96,72	107,25	132,65

Quelle: eigene Schätzungen.

9.5.3 Verlust von sicherheitssensiblen Kunden – Verschiebung der kommerziellen Nachfrage

Einige europäische Mobilfunknetzbetreiber sollten einkalkulieren, dass ein erheblicher Teil ihrer Kunden zu Mobilfunknetzbetreibern abwandert, die vertrauenswürdige Anbieter von 5G-Infrastrukturen nutzen. Steuereinnahmen und Arbeitsplätze könnten betroffen sein, wenn Kunden abwandern.

In Kapitel 6 haben wir beschrieben, wie wir die versteckten Kosten für Mobilfunknetzbetreiber abschätzen können, die dadurch entstehen, dass sicherheitsempfindliche Kunden ihr Geschäft zu anderen Betreibern - und sogar in andere Länder - verlagern. Zusammengefasst berechnen wir den Anteil der Umsätze von Mobilfunknetzbetreibern, der durch die Nutzung von Mobilfunkdiensten durch sicherheitsempfindliche Geschäftskunden entsteht.[153] Wir verwenden den BIP-Anteil von Anbietern kritischer Infrastrukturen und von IPR-intensiven Unternehmen als Näherungswert für sicherheitssensible Kunden.

149 Da für Portugal keine Daten zu den Kosten pro Sicherheitsverletzung vorliegen, gehen wir davon aus, dass, da die IKT-Branchen in Portugal und Italien einen ähnlichen prozentualen Anteil an der Wertschöpfung im Verhältnis zum BIP aufweisen, der Stand der Reaktionsfähigkeit und Kapazität in beiden Ländern ähnlich ist und der Unterschied bei den Kosten pro Sicherheitsverletzung proportional zur Größe des BIP beider Länder ist - Portugal etwa 12 % des italienischen Vergleichswert.

150 CNCS (2020), S. 40.

151 Berechnet aus US Dollar Werten bei einem Wechselkurs von 0,82€ zum Dollar.

152 In dieser Berechnung gehen wir davon aus, dass Frankreich im Verhältnis zu seiner Größe die gleichen Datenschutzverletzungen hat wie Deutschland. Dennoch hat Frankreich eine viel geringere Abhängigkeit von nicht-vertrauenswürdigen Netzwerken, weshalb die Kosten immer noch viel geringer sein dürften als in Deutschland.

153 Wenn keine internen Netzbetreiber-, Regierungs- und kommerziellen Informationen über den Anteil der Einnahmen oder Ausgaben dieser Kunden verfügbar sind, verwenden wir relevante Werte, wie z. B. den Anteil der sicherheitssensiblen Branchen am nationalen BIP, als vernünftige Annahmen, um unsere Berechnungen des Anteils der Einnahmen von diesen Kunden zu unterstützen.

Diese Verlagerung der Nachfrage wird die Gewinne der Mobilfunknetzbetreiber verringern und kann sogar Wohlfahrtsverluste für die gesamte Gesellschaft verursachen, je nachdem, ob die Kunden die Betreiber wechseln oder ihre gesamte Produktion in Länder mit sichereren Netzen verlagern. Die Zahlen könnten auch steigen, da zukünftige Regulierungen und Herausforderungen bei der Akquise von Versicherungen dazu führen könnten, dass selbst die Zulieferer der Kunden keine vertrauensunwürdigen 5G-Netze mehr nutzen.

- In **Deutschland** liegt der Anteil der Anbieter kritischer Infrastrukturen am BIP bei 27 %. Der Anteil der IPR-intensiven Wertschöpfung liegt bei fast 50 %. Wir schätzen daher, dass mehr als die Hälfte des Marktes mit Geschäftskunden und damit **4,6 Mrd. Euro** eine Tendenz zur Verlagerung hin zu Mobilfunknetzbetreibern mit ausschließlich vertrauenswürdiger Technologie in ihren 5G-Netzen haben werden. Die Kosten für Deutschland sind im Vergleich zu den drei folgenden Ländern deutlich höher, aufgrund einer breiteren Definition von KRITIS und einem höheren Anteil sowohl kritischer als auch IPR-intensiver Unternehmen.

- In **Frankreich** schätzen wir eine **Verschiebung der Nachfrage** im Wert von mehr als **1,2 Mrd. Euro** in einem Markt von 30,7 Mrd. Euro im Jahr 2020. Der Anteil der mobilen Telekommunikationsdienste am Umsatz ist ähnlich hoch wie in Deutschland (43 % vs. 44 % in Deutschland), aber die geschäftliche Nutzung ist etwas weniger als halb so hoch (18 % dieser 43 %), wobei bis zu 50 % der Geschäftskunden aus den KRITIS- und IPR-intensiven Bereichen kommen. Außerdem machen Betreiber, die nicht-vertrauenswürdige Geräte verwenden, nur ein Drittel des Geschäftskundenmarktes aus.

- In **Italien** könnten etwas mehr als **1,34 Mrd. Euro** des Umsatzes im Telekommunikationsmarkt durch eine Verschiebung der Nachfrage auf dem Spiel stehen. Italiens Markt im Jahr 2020 (31,58 Mrd. Euro) war weniger als halb so groß wie der deutsche, mit einem nur geringfügig höheren Anteil an Umsätzen, die durch mobile Telekommunikationsdienste generiert wurden (47,41 % gegenüber 43,97 %), und dem geringsten Anteil an Geschäftskunden (18 %) im Verhältnis zum Gesamtumsatz.

- In **Portugal** könnte der Telekommunikationsmarkt eine **Nachfrageverschiebung im Wert von bis zu 324,2 Mio. Euro** (oder 40 %) erleben. Diese Zahl könnte steigen, wenn die portugiesische Regulierung für die industrielle Cybersicherheit sensibler Sektoren aufholt. Portugal ist der kleinste Telekommunikationsmarkt unter den vier Ländern (3,55 Mrd. Euro im Jahr 2020), wenn auch mit dem größten Teilmarkt für mobile Telekommunikationsdienste.[154]

9.5.4 Verlust von sicherheitssensiblen Kunden - Verlagerung der Nachfrage der Regierung & redundante Infrastruktur

Regierungen müssen möglicherweise fast 700 Mio. Euro ausgeben, um sichere, redundante Netzwerke zu schaffen, wenn sie Mobilfunknetzbetreibern nicht vertrauen können, die Geräte nicht-vertrauenswürdiger Anbieter verwenden.

Regierungen haben eine weitere Möglichkeit, die Sicherheit der Netzwerke, auf die sie angewiesen sind, zu gewährleisten: den Aufbau eines eigenen Netzes. Natürlich ist dies extrem teuer und hängt von der Größe, der Anzahl der Knoten, den Sicherheitsanforderungen und den Funktionen ab, die es erfüllen muss, und bringt auch einen Aufschlag für einen staatlichen Kommunikationsanbieter oder zumindest unterbeauftragte Mobilfunknetzbetreiber für den Betrieb mit sich. Wir können die Kosten mit „Top-Down"-Methoden abschätzen, indem wir uns bestehende Projekte und analoge Initiativen aus der jüngeren Vergangenheit anschauen.

- Für **Deutschland** kostet ein nationales Notfallnetz – das Netz des Bundes – den Staat (Steuerzahler) bereits **mehr als 426 Mio. Euro** für die Umsetzung. Hinzu kämen jährliche Betriebskosten in Höhe von ca. 92 Mio. Euro/Jahr. Ursprüngliche Schätzungen des Bundes ergaben jedoch, dass ein externer Betreiber den Steuerzahler 160 Mio. Euro/Jahr kosten würde.

- Für **Frankreich** schätzen wir, dass das redundante Kommunikationsnetz, das derzeit in Betrieb ist,

154 Die sicherheitssensiblen Kunden machen den geringsten Anteil (20 %) des Telekommunikationsmarktes der vier von uns untersuchten Länder aus, was allerdings daran liegen mag, dass Portugals Definition der KRITIS-Sektoren sehr eng gefasst ist .

sogar noch mehr kostet als in Deutschland, möglicherweise bis zu **470 Mio. Euro oder mehr.**

- Für **Italien** schätzen wir, dass das Land bis zu **700 Mio. Euro** investieren muss. Italien ist eines der europäischen Länder mit der am besten entwickelten Zivilschutz- und Notfallinfrastruktur. Das Land hat mehrere Risiken (maritim, territorial usw.), daher gibt es eine relevante Anzahl von redundanten Notfallnetzen (UHF/CHF, Funk, TETRA usw.). In der Berechnung wurden diejenigen berücksichtigt, die laut Interview in Zukunft durch 5G ersetzt werden sollen, obwohl keine offiziellen Pläne bekannt gegeben wurden.

- **Portugal** hat bereits **450 Mio. Euro** in eine nationale Notfall-Telekommunikationsgesellschaft, SIRESP, investiert, die sich teilweise im Besitz der portugiesischen Regierung befindet. Um das 550-Antennen-Netz auf den neuesten Stand zu bringen, sind Verbesserungen der Robustheit und Sicherheit im Wert von etwa 25 Mio. Euro erforderlich. Portugal zahlt Altice und Motorola 30 Mio. Euro pro Jahr für den Betrieb des Netzes.

9.5.5 Kosten von Rip-and-Replace

Mobilfunknetzbetreiber und Regierungen lassen sich auf Haftungen in Milliardenhöhe ein, wenn größere Datenverluste oder zwischenstaatliche Konflikte das Entfernen und Ersetzen von nicht-vertrauenswürdigen 5G-Netzen erfordern.

„Rip-and-Replace" ist ein Kostenfaktor für Mobilfunknetzbetreiber und möglicherweise deren Kunden, eine Anforderung, die sich im Allgemeinen aus Änderungen der nationalen Gesetzgebung ergibt. In Frankreich gibt es bereits Rip-and-Replace-Anordnungen für Bouygues und SFR. Rip-and-Replace wird zweifelsohne nach größeren Serviceausfällen oder Angriffen durch nicht-vertrauenswürdige Anbieter erforderlich sein.

Die Kosten hängen von der Größe des Staates, der Verankerung von nicht-vertrauenswürdigen Anbietern in der Infrastruktur und den Zeitspannen ab, in denen Rip-and-Replace erforderlich ist. Beispielsweise ist ein kurzfristiges, überstürztes Rip-and-Replace nach absichtlichen Störungen oder Serviceausfällen wahrscheinlich viel teurer als ein langfristiges, geordnetes Rip-and-Replace, das vom Gesetzgeber vorgeschrieben ist. Der Austausch von 5G-Infrastrukturen ist ein Kostenfaktor, der weiter eskalieren wird, je weiter Geräte nicht-vertrauenswürdiger Anbieter in eine nationale 5G-Infrastruktur eingebettet sind. Für erste Schätzungen haben wir zitierte Zahlen von Mobilfunknetzbetreibern und bestehende Berichte verwendet. Die Zahlen decken keine zusätzlichen Entschädigungen ab.

Die Dt. Telekom behauptet, dass es sie **ca. 3 Mrd. Euro kosten würde, Geräte von nicht-vertrauenswürdigen Anbietern auszumustern und zu ersetzen.**[155] Diese Zahl können wir nicht verifizieren, aber sie scheint die Kosten für den Wechsel zu einem vertrauenswürdigen Anbieter stark zu übertreiben. So beziffert beispielsweise British Telecom, die ebenfalls sehr stark auf Huawei-Technik gesetzt hat, die Kosten für ein vollständiges Verbot auf nur 500 Mio. Pfund.[156] Es scheint, als ignoriere die Deutsche Telekom in ihrer Kalkulation die Kosten, die später im Lebenszyklus ihres 5G-Netzes entstünden, wenn dieses mit nicht-vertrauenswürdiger Technik gebaut würde. Und natürlich ignoriert ein Mobilfunknetzbetreiber bei seiner Kalkulation die Kosten, die von anderen getragen werden müssen.

In **Frankreich** können wir **Kosten von bis zu 1 Mrd. Euro erwarten**, was die etwas geringere Marktgröße und die Dominanz der Infrastrukturen von Ericsson und Nokia widerspiegelt.[157] In **Italien** erwarten wir Kosten in Höhe von **etwa 600 Mio. Euro**, die aus einer 2019 erstellten Studie hervorgehen[158]. Für **Portugal** konnten wir keine ähnliche Schätzung für die Kosten für den Ersatz von nicht-vertrauenswürdiger Technik aus 4/5G-Netzen finden.

155 Handelsblatt (2020).
156 Reuters (2020).
157 Le Figaro (2020).
158 Bechis (2020), Istituto Affari Internazionali (2020).

TABELLEN- UND ABBILDUNGSVERZEICHNIS

Abbildung 1: 5G wird niedrige Latenzzeiten und hohen Durchsatz bei allen Diensten unterstützen 13

Abbildung 2: Staatliche und private Bereitstellung von Sicherheit 26

Abbildung 3: Anzahl der Data Breaches 2019-2020 51

Abbildung 4: Skalierung der Schäden für Frankreich und Italien (Euro) 67

Abbildung 5: Skalierung der Schäden für Portugal (Euro) 67

Abbildung 6: Skalierung der Schäden für Deutschland (Euro) 68

Tabelle 1: Art der versteckten Kostenkategorien – externe und Lebenszykluskosten 6

Tabelle 2: Entwicklung der Mobilfunknetze – Up- und Downloadgeschwindigkeiten 11

Tabelle 3: Technische Merkmale und Vorteile von 5G im Vergleich zu 4G 12

Tabelle 4: Systemanforderungen aus Anwendungsfällen und technischer Realisierung in 5G 17

Tabelle 5: Geschätzte Kosten eines Totalausfalls des Kommunikationsnetzes 25

Tabelle 6: Erwartete jährliche Kosten für die Einhaltung ausgewählter Vorschriften (deutsche Beispiele) 38

Tabelle 7: Mögliche Verschiebung der Nachfrage kritischer Infrastrukturindustrien weg von MNOs, die nicht-vertrauenswürdige Netzwerke betreiben 36

Tabelle 8: Potenzielle Verschiebung der Nachfrage von Industrien, die geistige Eigentumsrechte benötigen, weg von Mobilfunknetzbetreibern, die nicht vertrauenswürdige Netzwerke betreiben 43

Tabelle 9: Wahrscheinliche zukünftige Präsenz von nicht vertrauenswürdigen Anbietern in 5G-Infrastrukturen 58

Tabelle 10: Voraussichtlicher Anstieg der nationalen Kosten für Datenschutzverletzungen, die über ein nicht vertrauenswürdiges 5G-Netzwerk auftreten 70

LITERATURVERZEICHNIS

5G PPP Security WG (no year): "5G PPP Security Phase 1 Security Landscape", https://usermanual.wiki/Document/5GPPPWhitePaperPhase1SecurityLandscapeJune2017.809074850/view, [Dezember 2020].

Akerlof, George A. (1970), „The Market for ‚Lemons': Quality Uncertainty and the Market Mechanism". Quarterly Journal of Economics. The MIT Press.

ASPI (2020): "ICT for Development in the Pacific Islands", https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-02/ICT%20for%20development%20in%20the%20Pacific%20islands.pdf?x_oS.r8OVVfTlxxgNHI58k_VL45KC83H, [Oktober 2020]

Behesti, B. (2019): "What 5G means for smart cities", London, https://www.smartcitiesworld.net/opinions/opinions/what-5g-means-for-smart-cities, [Oktober 2020].

Berzina, Kristine (2020): 5G Security: The New Energy Security. Europe's Strategic Vulnerabilities in the 5G Era and Lessons Learned from Europe's Dependence on Russia's Natural Gas. https://securingdemocracy.gmfus.org/5g-energy-security , [November 2020].

Bischoff, P. (2020): "How data breaches affect stock market share prices", Kent, https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/, [Oktober 2020].

Bitkom (2018): "Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie", Studienbericht 2018, https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, [August 2020].

BMI (2020): "Bundesministeriums des Innern, für Bau und Heimat: Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0), 19. November 2020, Berlin.

BMWi (2018): "KfW erwirbt im Auftrag des Bundes temporär Anteil am deutschen Übertragungsnetzbetreiber 50Hertz", https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2018/20180727-kfw-erwirbt-im-auftrag-des-bundes-temporaer-anteil-am-deutschen-uebertragungsnetzbetreiber-50hertz.html, [Oktober 2020].

Brookings Institution (2017): „Global digital trade 1: Market opportunities and key foreign trade restrictions". Testimony of Joshua P. Meltzer before the United States International Trade Commission, April 12, 2017, https://www.brookings.edu/testimonies/global-digital-trade-1-market-opportunities-and-key-foreign-trade-restrictions/ , [Dezember 2020].

Bretschneider, W., Freytag, A., Rieckmann, J., Stuchtey, T. (2020): Sicherheitsverantwortung zwischen Markt und Staat – eine institutionentheoretische Analyse, in: ORDO, Vol. 70 Nr. 1, S. 89 – 124.

BSI (2020): "Zertifizierung und Anerkennung", Bonn, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/ITSEC_CC/CC_Liste/CC_Liste_node.html, [Oktober 2020].

Bughin, J. et al (2016): "Digital Europe: Pushing the Frontier, Capturing the Benefits", McKinsey Global Institute, Juni 2016.

Bundesnetzagentur (2020): "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0", S. 9 – 10, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Katalog-Sicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=3 , [November 2020].

Bundesamt für Verfassungsschutz (2019): "Verfassungsschutzbericht 2019", https://www.verfassungsschutz.de/embed/vsbericht-2019.pdf

Busse, M. and C. Hefeker (2007): "Political risk, institutions and foreign direct investment". European Journal of Political Economy 23, 397-415

Cave, D. (2020): "5G matters: (Geo)politics and critical national infrastructure", https://www.orfonline.org/expert-speak/5g-matters-geopolitics-critical-national-infrastructure-60548/, [Oktober 2020]..

Cerulus L. (2019): "How Ukraine became a test bed for cyberweaponry", https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/, [Oktober 2020].

CNCS (2020), "Ciberseguranca em Portugal – Riscos & Conflitos", https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriocibersegurança_cncs.pdf, [Dezember 2020].

Commission ad hoc Cyber Risk (2018): "Assurer le risque cyber - Rapport du Club des juristes", https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_assurer-le-risque-cyber_janvier_2018_fr-2.pdf, [November 2020].

Cotelle, P., Wolf, P., Suzan, B., Santoni, J.L., Lemerle, L. et al. (2019): "Maîtrise du Risque Cyber et Assurance : Scénario cyber s'appliquant à la filière aéronautique Réponse du marché", Rapport de recherché, IRT SystemX.

Cotelle, P., Wolf, P., Suzan, B. (2015): "Cyber Risk and Insurance Cyber Risk Governance throughout the value chain and its transfer to the Insurance", Cyber Risk and Insurance, https://www.irt-systemx.fr/wp-content/uploads/2017/01/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang-v2.pdf, [Oktober 2020].

Crawford, N. (2020): "Defending against economic statecraft: China, the US and the rest", https://www.iiss.org/blogs/analysis/2020/10/economic-statecraft-china-us, [Oktober 2020].

CrowdStrike (2019): "CrowdStrike Report Reveals Cyber Intrusion Trends from Elite Team of Threat Hunters", October 9, 2019, at https://www.crowdstrike.com/resources/news/crowdstrike-report-reveals-cyber-intrusion-trends-from-eliteteam-of-threat-hunters/, [Oktober 2020].

Defense Science Board (2019): "Defense Applications of 5G Network Technology", https://www.hsdl.org/?abstract&did=828623#:~:text=From%20the%20Executive%20Summary%3A%20%22Emerging,4G%20%5Bfourth%20generation%5D%20networks, [Oktober 2020].

Demer, John C. (2018): U.S. Department of Justice, Statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice Before the Committee on the Judiciary, United States Senate, December 12, 2018, unter https://www.judiciary.senate.gov/imo/media/doc/12-12-18%20

Demers%20Testimony.pdf

Department of Defense (DoD). (2020): "Department of Defense (DoD) 5G Strategy", https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf , [Oktober 2020].

Deutsche Bundesbank (2012): "Kalendarische Einflüsse auf das Wirtschaftsgeschehen", Monatsbericht Dezember, S.59.

DG Connect (2020), "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures". https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures, [Oktober 2020].

DLA Piper (2020): "DLA Piper GDPR data breach survey 2020", https://www.dlapiper.com/en/uk/insights/publications/2020/01/gdpr-data-breach-survey-2020/, [Dezember 2020].

Ekudden, Erik (2018): "Five Technology Trends Augmenting the Connected Society", in: Ericsson Technology Review, September 10, 2018, https://www.ericsson.com/48f8e0/assets/local/reports-papers/ericsson-technology-review/docs/2018/technology-trends-2018.pdf.

Endgadget (2020): "Huawei tested facial recognition that targeted Uyghurs in China". December 8, 2020, https://www.engadget.com/huawei-facial-recognition-uyghurs-172304197.html?guccounter=2 , [Dezember 2020].

Ericsson (2019): "What role will Artificial Intelligence have in the mobile networks of the future?", https://www.ericsson.com/en/networks/offerings/network-services/ai-report, [Oktober 2020].

Ericsson (2020a). "Security in 5G RAN and Core deployments", https://www.ericsson.com/49a5ea/assets/local/reports-papers/white-papers/ericsson-whitepaper-5gran.pdf, [November 2020].

Ericsson (2020b): "TDC Denmark goes live with Ericsson 5G", https://www.ericsson.com/en/news/2020/9/tdc-denmark-goes-live-with-ericsson-5g, [Oktober 2020].

Ericsson (2020c): "5 Key Facts About Radio Access Networks", https://www.ericsson.com/en/public-policy-and-government-affairs/5-key-facts-about-5g-radio-access-networks, [Oktober 2020].

ENISA (2018): "Signaling Security in Telecom SS7/Diameter /5G", https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport, [Oktober 2020].

EU Commission (2020): Commission Staff Working Document, "Report on the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks", SWD (2020) 357 final.

European Union Agency for Cyber Security (ENISA) (2019): "Threat Landscape for 5G Networks", https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, [Oktober 2020].

European Union Intellectual Property Office (EUIPO) (2019): "Impact of intellectual property rights intensive industries in the European Union", https://euipo.europa.eu/ohimportal/en/web/observatory/ip-contribution, [November 2020].

Bundesrat (2016): Entwurf eines Zweiten Gesetzes zur Änderung des BDBOS-Gesetzes, Drucksache 786/16 (neu).

Bundesgesetzblatt (2020): Gesetzüber die Feststellung eines Zweiten Nachtrags zum Bundeshaushaltsplan für das Haushaltsjahr 2020 (Zweites Nachtragshaushaltsgesetz 2020).

Financial Times (2020a): "China's biggest chipmaker SMIC hit by US sanctions", https://www.ft.com/content/7325dcea-e327-4054-9b24-7a12a6a2cac6?shareType=nongift, [Oktober 2020].

Financial Times (2020b): "Germany crackdown set to exclude Huawei from 5G rollout", https://www.ft.com/content/35197477-acef-4429-a1d8-71743ee8d8e3, [Oktober 2020].

Fraunhofer IIS (2020): "Staatsminister Aiwanger eröffnet 5G Bavaria-Testzentrum und das Testbed-Industrie 4.0 am Fraunhofer IIS", Erlangen, https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf, Zugriff 2020.

Gambetta, Diego (1988): 'Can We Trust Trust?' in: D.G. Gambetta (ed.) Trust, New York: Basil Blackwell: 213–37.

Bundesrechnungshof (2017): "Jahresbericht 2017", Einzelplanbezogene Prüfungsergebnisse, Bundesministerium des Innern, Bemerkungen No. 04 S.2, https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/bemerkungen-jahresberichte/jahresberichte/2017/einzelplanbezogene-pruefungsergebnisse/bundesministerium-des-innern, [Oktober 2020].

Gilli, A & Bechis, F. (2020): "NATO & the 5G Challenge", https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html , [Oktober 2020].

Globaltrademag.com (2020): Unpacking US-China Sanctions and Export Control Regulations: Huawei. Sept. 10,2020, https://www.globaltrademag.com/unpacking-us-china-sanctions-and-export-control-regulations-huawei/, [Oktober 2020].

GSMA (2019): „The 5G Guide – A Reference for Operators", https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf, [November 2020].

Hammami, H., Hammami, M., Coulibaly, S., & Marzouk, M. (2020): "Determinants of FDI attractiveness: A MCI model approach". Economics Bulletin, 40(2), 1033-1048.

Handelsblatt (2014): "Bund baut Kommunikationssystem um", Handelsblatt from the 26th June, https://www.handelsblatt.com/politik/deutschland/nach-nsa-affaere-bund-baut-kommunikationsnetz-um/10114010.html?ticket=ST-1479718-bbBLRnwCBze-AYJsKvdb0-ap2, [Oktober 2020]..

Handelsblatt (2020): „„Armageddon"-Szenario: Telekom spielt Huawei-Bann durch", https://www.handelsblatt.com/technik/it-internet/ausschluss-von-netzausruester-armageddon-szenario-telekom-spielt-huawei-bann-durch/25918402.html?ticket=ST-2101572-caqXUFPkiY5AFBKX0pz2-ap4, [November 2020].

Hansen, A. und Meyer, D. (2018): "Wie viel kosten uns die arbeitsfreien Feiertage?", ifo Schnelldienst Kommentar, März, S.18.

Herpig, Sven (2020): Understanding The Security Implications Of The Machine-Learning Supply Chain. Available at: https://www.

LITERATURVERZEICHNIS

stiftung-nv.de/sites/default/files/understanding_the_security_of_the_machine-learning_supply_chain.pdf, [Oktober 2020].

Holland, M. (2014): "NSA-Skandal: Auch Bundestag beendet Kooperation mit Verizon", https://www.heise.de/newsticker/meldung/NSA-Skandal-Auch-Bundestag-beendet-Kooperation-mit-Verizon-2241967.html, [Oktober 2020].

Hui, X et al. (2020): "5G network-based Internet of Things for demand response in smart grid: A survey on application potential", Applied Energy, Vol. 257. https://www.sciencedirect.com/science/article/pii/S0306261919316599 , [Oktober 2020].

IBM (2020): "Cost of a Data Breach Report", November 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/ , [Oktober 2020].

Information is beautiful (2020): "Codebases – Millions of lines of code", https://informationisbeautiful.net/visualizations/million-lines-of-code/, [Oktober 2020].

International Telecommunications Union (ITU) (2018): "Setting the Scene for 5G: Opportunities & Challenges", Switzerland, https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf

ITU (2019): „Financial Inclusion Global Initiative (FIGI)", Report of Security Workstream, https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20the%20SS7%20vulnerabilities%20and%20their%20impact%20on%20DFS%20transactions.pdf, [Oktober 2020].

Jornaldenegocios (2020): "Centeno: Queda do PIB é de 6,5% por cada 30 dias úteis com economia parada". https://www.jornaldenegocios.pt/economia/detalhe/centeno-queda-do-pib-e-de-65-por-cada-30-dias-uteis-com-economia-parada , [Dezember 2020].

Kavanagh, S. (n.a): "What is Enhanced Mobile Broadband?", United Kingdom, https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/ , [Oktober 2020].

Kim, B. (2019): "ICT-Based Business Communication with Customers in the 4th Industrial Revolution Era", Business Communication Research and Practice, 2(2), p. 55-61.https://doi.org/10.22682/bcrp.2019.2.2.55 , [Oktober 2020].

KPMG (2019): "Cloud-Monitor 2019 - Public Cloud und Cloud Security sind kein Widerspruch", https://hub.kpmg.de/cloud-monitor-2019, [Oktober 2020].

Lee, J. (2019): "The National Security Risks Over Huawei and its 5G Network: Is an Outright Ban or a Restricted Access the Answer?", Oxford, https://www.law.ox.ac.uk/research-subject-groups/commercial-law-centre/blog/2019/05/national-security-risks-over-huawei-and, [Oktober 2020].

Le Figaro (2020): "5G sans Huawei: l'État négocie avec les opérateurs", 6.3.2020, https://www.lefigaro.fr/secteur/high-tech/5g-sans-huawei-l-etat-negocie-avec-les-operateurs-20200306#_=_, [Dezember 2020].

Le Maistre, R. (2020): "Rakuten, Telefónica join forces on Open RAN developments", https://www.telecomtv.com/content/open-networking/rakuten-telef-nica-join-forces-on-open-ran-developments-39678/, [November 2020}.

Lewis, J. (2018): "How 5G will shape innovation and security", Washington DC, https://csis-website-prod.s3.amazonaws.com/s3fs: -public/publication/181206_Lewis_5GPrimer_WEB.pdf, [Oktober 2020].

Lloyds (2015): "Business Blackout: The insurance implications of a cyber attack on the US power grid", Cambridge, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloyds-business-blackout-scenario.pdf, [Oktober 2020].

Lord, N. (2019): "Data Protection: Data In Transit vs. Data At Rest", https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest, [Dezember 2020].

Miller, M. (2020): "Defense Department designates $600 million for 5G testing at military sites", Washington DC, https://thehill.com/policy/technology/520288-defense-department-designates-600-million-for-5g-testing-at-military-sites , [Oktober 2020].

Nakashima, E. (2019): "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", Washington DC, Washington Post from the 29th May, 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, accessed Oct. 2020.

NIS Cooperation Group (2020): "Cybersecurity of 5G networks – EU toolbox of risk mitigating measures", CG Publication, January, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Nokia (2020a): "Connected Vehicles", https://www.nokia.com/networks/5g/use-cases/connected-vehicles/ , [Oktober 2020].

Nokia (2020b): "E-Health", https://www.nokia.com/networks/5g/use-cases/ehealth/ , Zugriff im Okt 2020.

Nokia (2020c): "Threat Intelligence Report 2020", https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html?_ga=2.263942024.520766677.1603877763-652481011.1603877763, [Oktober 2020].

Normenkontrollrat (2014): „Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 3044)", 4. December 2014, Berlin.

Normenkontrollrat (2016): „Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NKR-Nummer 3970, BMI)".

NCSC (2020): "Security analysis for the UK telecoms sector", Summary of findings, https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf, [Oktober 2020].

Okumura Y. (2019): "5G for eHealth – 5G Utilization in Telemedicine", ITU-D Study Groups Rapporteur Group meetings, https://www.itu.int/dms_pub/itu-d/oth/07/1e/D071E0000010001PDFE.pdf , [Oktober 2020].

Owen, G. (2020): "The race to Open RAN is a marathon, not a

sprint", https://www.huawei.com/en/publications/communicate/89/open-ran-is-a-marathon-not-a-sprint, accessed Oct 2020.

Oxford Economics (2020): "Restricting Competition in 5G Network Equipment Throughout Europe – an Economic Impact Study", June 2020.

Park, J.-Y., Robles, R., Hong, C.-H., Yeo, S.-S., & Kim, T.-h. (2008): "IT Security Strategies for SME's", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, pp. 91-98.

Ponemon Institute (2017): "The impact of data breaches on reputation and share value", https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf, [Oktober 2020].

Prague 5G Security Conference (2019): "The Prague Proposals", Prague, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/, [Oktober 2020].

Prague Proposals (2019): https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf, [Oktober 2020].

Pupillo, L. (2019): "5G and National Security: A complex puzzle", Brussels, https://www.ceps.eu/5g-and-national-security/, Oct 2019.

Reuters (2020): "BT says Huawei ban can be absorbed in 500 million pounds already earmarked", https://www.reuters.com/article/us-britain-huawei-bt-costs/bt-says-huawei-ban-can-be-absorbed-in-500-million-pounds-already-earmarked-idUSKCN24F2A2, [Dezember 2020].

Roke Manor Research Ltd (2020): "5G & Law Enforcement: How it could impact investigation & crime prevention", Hampshire, https://www.roke.co.uk/media/dtwinm2g/5g-law-enforcement-article-long-final-whitepaper-template.pdf , [Oktober 2020].

Sachverständigenrat (2016): "Jahresgutachten 2016/2017: Zeit für Reformen", https://www.sachverstaendigenrat-wirtschaft.de/fileadmin/dateiablage/gutachten/jg201617/ges_jg16_17.pdf, [Oktober 2020].

Sachverständigenrat (2019): „Jahresgutachten 2019/2020: Den Strukturwandel meistern", https://www.sachverstaendigenrat-wirtschaft.de/jahresgutachten-2019.html, [Oktober 2020].

Säkerhetspolisen (2020): "The importance of a secure 5G network", Stockholm, https://www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2020-10-20-the-importance-of-a-secure-5g-network.html?utm_campaign=21.%20october%202020%20-%20Kundeemneliste%20-%20What%20creates%20competition%20in%20the%20telecommunications%20industry%20Can%20the%20number%20of%20mobile%20operat189115&utm_source=Kundeemneliste&utm_medium=email, [Oktober 2020].

Shermann, J. (2019): https://medium.com/dukeuniversity/whats-the-deal-with-huawei-and-a-hack-at-african-union-headquarters-1e454c1f31a2, [November 2020].

Sivalingum, T, et al. (2019): "Positioning of Multiple Unmanned Aerial Vehicle Base Stations in future Wireless Network", Oulu, https://www.researchgate.net/publication/335826943_Positioning_of_Multiple_Unmanned_Aerial_Vehicle_Base_Stations_in_future_Wireless_Network , [Oktober 2020].

Smartbear (2019): "Bewährte Verfahren für die Codeprüfung", https://smartbear.com/learn/code-review/best-practices-for-peer-code-review/?lang=de-de, [Oktober 2020].

Statistisches Bundesamt (2020): "Federal Statistical Office: National accounts, gross domestic product 2019", Wiesbaden, https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Tabellen/bip-bubbles.html, [Oktober 2020].

Strand Consult (2019): "The real cost to rip and replace of Chinese equipment in telecom networks", https://strandconsult.dk/the-real-cost-to-rip-and-replace-chinese-equipment-from-telecom-networks/, [Oktober 2020].

Strand Consult (2020): "Understanding the Market for 4G RAN in Europe", https://strandconsult.dk/understanding-the-market-for-4g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-102-mobile-networks/ , [Oktober 2020].

Sullivan, J. and Kamensky, D. (2017): "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid", The Electricity Journal, 30(3), pp. 30-35.

Taulli, T. (2020): "How 5G will unleash AI", https://www.forbes.com/sites/tomtaulli/2020/05/08/how-5g-will-unleash-ai/ , [Oktober 2020].

techUK. (2019): "How can 5G technology support the emergency services?", https://www.techuk.org/insights/reports/item/15317-report-how-can-5g-technology-support-the-emergency-services , [Oktober 2020].

The Australian Financial Review (2020) Huawei data centre built to spy on PNG. https://www.afr.com/companies/telecommunications/huawei-data-centre-built-to-spy-on-png-20200810-p55k7w, [Oktober 2020].

thelocal.dk (2020): "Denmark's TDC shuns China's Huawei for 5G rollout", Stockholm, https://www.thelocal.dk/20190319/denmarks-tdc-shuns-chinas-huawei-for-5g-rollout, [Oktober 2020].

Tomás, J. P. (2020): "Rakuten Mobile launches 5G services in parts of Japan", RCRWireless News from the 30th September, https://www.rcrwireless.com/20200930/5g/rakuten-mobile-launches-5g-services-in-parts-of-japan.

U.S. Department of Commerce (2020): Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies. Press release, May 15, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts, [Oktober 2020].

UTAIL (2020): "Custa Quanto? Regulamento (EU) 2016/679 (Regulamento Geralde Proteção de Dados (RGPD))" https://www.jurisapp.gov.pt/media/1109/ail-rgpd.pdf , [Oktober 2020].

Voland, T. and Büsch, P. (2020): "Nächster Versuch – BMI legt neuen Entwurf des IT SiG 2.0 vor", https://www.politik-kommunikation.de/gesetz-des-monats/naechster-versuch-bmi-legt-neuen-entwurf-des-it-sig-20-vor-1781324920#:~:text=W%C3%A4hrend%20die%20strafrechtlichen%20Vorschriften%20aus,Erh%C3%B6hung%20der%20m%C3%B6glichen%20Bu%C3%9Fgeldzahlungen%20vor, [Oktober 2020].

LITERATURVERZEICHNIS

Wagener, T. (2020): „Low Economic Cost of Excluding Huawei and ZTE in European Markets," U.S. Department of State Office of the Chief Economist Working Paper, November.

Wang, Z. (2019): "Systematic Government Access to Private-Sector Data in China", https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11, [Oktober 2020].

Watts, J. (2019): "A framework for an open, trusted, and resilient 5G global telecommunications network", https://www.atlanticcouncil.org/in-depth-research-reports/report/a-framework-for-an-open-trusted-and-resilient-5g-global-telecommunications-network/#stateofcompetitionandrisk, [Oktober 2020].

Washington Post (2020): "Huawei tested AI software that could recognize Uighur minorities and alert police, report says". https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/ , [Dezember 2020].

Wheeler, T. and Simpson, D. (2019): "Why 5G requires new approaches to cybersecurity", https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/, [Oktober 2020].

Williams, C. (2020): "Espionage and the race for a coronavirus vaccine", Canberra, https://www.canberratimes.com.au/story/6841183/espionage-and-the-race-for-a-covid-19-vaccine/, [Oktober 2020].

Winder, Davey (2019): Texas Cyber Attack has taken 23 Government Agencies Offline, in: Forbes, Aug. 19, 2019, https://www.forbes.com/sites/daveywinder/2019/08/19/texas-cyber-attack-has-taken-23-government-agencies-offline/?sh=7840aab32d65, [Oktober 2020].

World Bank (2020): "World Bank Open Data ". https://data.worldbank.org/, accessed Dec. 2020.

World Economic Forum (2020): "The Impact of 5G: Creating New Value across Industries and Society", Switzerland, http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf , [Oktober 2020].

World Justice Project (2020): "WJP Rule of Law Index 2020", https://worldjusticeproject.org/, [Oktober 2020].

Xi JinPing (2015): Ministry of Foreign Affairs of the People's Republic of China, Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference, December 16, 2015, , [Oktober 2020].

AUTOREN

Prof. Dr. Christian Dörr studierte Informatik und Betriebswirtschaft an der Universität Paderborn und promovierte in Informatik und Kognitionswissenschaften an der University of Colorado at Boulder, USA. Er ist Professor für Cybersicherheit und Unternehmenssicherheit am Hasso-Plattner-Institut für Digital Engineering und an der Universität Potsdam. Seine Kernkompetenzen sind Netzwerk- und Kommunikationssicherheit, Cyber Threat Intelligence und Schutz kritischer Infrastrukturen.

Dr. Enrico Frumento ist Domain-Spezialist im Cybersecurity-Team von Cefriel, einem europäischen und privat finanzierten Forschungs- und Innovationsprojekt zur ICT-Sicherheit. Er ist Autor von themenbezogenen Publikationen und Büchern und Mitglied der European CyberSecurity Organisation. Seine mehr als 20-jährige Forschungstätigkeit konzentriert sich auf unkonventionelle Sicherheit, Technologien, Taktiken und Techniken zur Aufklärung von Cyberkriminalität, den Gegensatz zum modernen Social Engineering und die dynamische Bewertung der Schwachstellen von Organisationen, die gefährdeten materiellen und immateriellen Werten entsprechen.

Carlos Oliveira hat einen MsC in Software-Engineering von der Universität Coimbra. Er ist Head of New Ventures bei Ubiwhere, einem Unternehmen, das sich seit seiner Gründung auf Future Internet Technologies und Smart City Plattformen konzentriert. Carlos hat auch als Senior Product Manager mit großen datenintensiven Verbraucherprodukten gearbeitet, wodurch er sich mit den praktischen Auswirkungen der Handhabung und Sicherung großer Mengen von Verbraucherinformationen befasst hat, und verfügt über langjährige Erfahrung in F&E- und kommerziellen Projekten im Telekommunikationssektor.

Gianmarco Panza ist Senior Domain-Spezialist in den verschiedenen Bereichen der Vernetzung bei Cefriel, einem europäischen und privat finanzierten Projekt für F&E und Innovationen. Er hat einen Abschluss in Information Science Engineering von der Universität Padua und einen Master-Abschluss in ICT von Cefriel/Politecnico di Milan. Er unterrichtet in ICT-Masterkursen und bei der Schulung von Firmenmitarbeitern über Netzwerke der nächsten Generation. Er hat mehrere IEEE-Publikationen in den Bereichen Digital Signal Processing und Networking und ist ein Senior IEEE Member. Seine Kompetenzen erstrecken sich von der Planung und dem Design bis hin zum Testen und zur Validierung und decken auch die neuartigen Dienste ab, die durch die nächste Generation von Netzwerken, wie 5G und darüber hinaus, ermöglicht werden.

Stefan Rausch hat einen MA in Politikwissenschaft und ist Spezialist für Regierungsbeziehungen und Projektmanager bei der Public-Affairs-Beratung Rubis Development Group mit Schwerpunkt auf Verteidigungs-, Sicherheits- und cyberbezogenen Themen. Er hat Politikwissenschaft, Kommunikation und Area Studies in Rostock und Tallinn studiert und arbeitete am Lehrstuhl für Vergleichende Politikwissenschaft der Universität Rostock, bevor er 2015 zur Rubis DGroup kam.

Dr. Johannes P. Rieckmann studierte Volks- und Betriebswirtschaftslehre in Bremen und Paris und promovierte in Entwicklungsökonomie an der Universität Göttingen. Er ist Senior Research Fellow am BIGS und Alumni-Forschungsstipendiat des DAAD-AICGS.

Dr. Tim H. Stuchtey studierte Volkswirtschaftslehre an der Westfälischen Wilhelms-Universität Münster und promovierte in Volkswirtschaftslehre an der Technischen Universität Berlin. Er ist Direktor des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS), einem Think Tank für zivile Sicherheit mit Fokus auf ökonomische Aspekte der Sicherheit mit Sitz in Potsdam. Tim Stuchtey ist außerdem ein Non-Resident Fellow am American Institute for Contemporary German Studies (AICGS) in Washington, DC..

Dr. Reda Yaich ist Senior Researcher und Leiter des Cybersecurity-Teams am IRT SystemX. Er hat einen Doktortitel in Informatik von der ENS Mines in Saint-Etienne mit einem Schwerpunkt auf Vertrauensmanagement unter Verwendung von Technologien der künstlichen Intelligenz. Er war als Dozent und/oder Forschungsassistent an mehreren Universitäten (z.B. Universität Saint-Etienne, Universität Lyon) und Ingenieurschulen (ENS Mines Saint-Etienne, Telecom Bretagne, IMT Atlantique, ENSIBS, Telecom SudParis) tätig. Reda Yaich hat mehrere Veröffentlichungen in Fachzeitschriften und auf Konferenzen im Zusammenhang mit dezentraler Zugriffskontrolle, Autorisierung und digitalem Vertrauensmanagement.

BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Das Brandenburgische Institut für Gesellschaft und Sicherheit ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes Institut in Potsdam mit der Mission, Brücken zwischen Theorie und Praxis zu bauen, um durch seinen multi- und interdisziplinären Ansatz einen Beitrag zur Stärkung der zivilen Sicherheit zu leisten.

Located in Potsdam, the Brandenburg Institute for Society and Security is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security.

www.bigs-potsdam.org