DE 2022

03

Sonderbericht

5G-Einführung in der EU:

Verzögerungen beim Auf- und Ausbau der Netze und ungelöste Sicherheitsprobleme

CURIA RATIONUM

EUROPÄISCHER RECHNUNGSHOF

Inhalt

Zusammenfassung

I Die "fünfte Generation" von Telekommunikationssystemen, kurz 5G, ist ein neuer globaler Funkstandard, der eine deutlich höhere Datenkapazität und Übertragungsgeschwindigkeit bietet. 5G-Dienste sind eine wesentliche Voraussetzung für vielfältige innovative Anwendungen, die in vielen Bereichen unserer Wirtschaft einen Wandel nach sich ziehen und im Alltag der Bürgerinnen und Bürger Verbesserungen mit sich bringen können. 5G ist daher für den gesamten Binnenmarkt von strategischer Bedeutung.

II In ihrem 5G-Aktionsplan von 2016 hat die Kommission die Gewährleistung einer lückenlosen 5G-Abdeckung in städtischen Gebieten und entlang der wichtigsten Verkehrswege bis 2025 als Ziel vorgegeben. Im März 2021 weitete sie das Ziel der 5G-Abdeckung auf alle besiedelten Gebiete bis 2030 aus.

III 5G bietet viele Wachstumschancen, birgt aber auch gewisse Risiken. In ihrer Empfehlung zur 5G-Cybersicherheit aus dem Jahr 2019 warnte die Kommission, dass die Folgen weitverbreiteter Störungen aufgrund der Abhängigkeit vieler kritischer Dienste von 5G-Netzen besonders gravierend seien. Aufgrund des grenzübergreifenden Charakters der betreffenden Bedrohungen würden sich alle erheblichen Schwachstellen und Cybersicherheitsvorfälle in einem Mitgliedstaat zudem auf die Union als Ganzes auswirken. Eines der Ergebnisse der Empfehlung der Kommission war das im Januar 2020 angenommene EU-Instrumentarium für die 5G-Cybersicherheit ("5G-Toolbox").

IV Die Gesamtkosten der 5G-Einführung in der gesamten EU könnten sich auf 400 Milliarden Euro belaufen. Im Zeitraum 2014-2020 stellte die EU für 5G-Projekte Mittel in Höhe von über 4 Milliarden Euro bereit.

V Der Hof untersuchte, ob die Kommission die Mitgliedstaaten wirksam dabei unterstützt hat, die EU-Ziele für den Ausbau ihrer 5G-Netze zu erreichen und sich in abgestimmter Weise mit Sicherheitsbedenken hinsichtlich 5G auseinanderzusetzen. Der Hof bewertete Aspekte im Zusammenhang mit der Einrichtung von 5G-Netzen, für die das Jahr 2020 von entscheidender Bedeutung war, sowie mit deren Sicherheit. Mit diesem Bericht sollen Erkenntnisse und Empfehlungen für die zügige Einführung sicherer 5G-Netze in allen EU-Ländern bereitgestellt werden. Bei seiner Prüfung richtete der Hof seinen Fokus auf die Kommission, berücksichtigte aber auch die Rolle der nationalen Verwaltungen und anderer Akteure.

VI Die Prüfung des Hofes ergab, dass es bei der Einführung der 5G-Netze in den Mitgliedstaaten zu Verzögerungen kommt. Bis Ende 2020 hatten 23 Mitgliedstaaten kommerzielle 5G-Dienste eingeführt und das Zwischenziel von mindestens einer Großstadt mit 5G-Zugang erreicht. Allerdings sind nicht in allen 5G-Strategien oder Breitbandplänen der Mitgliedstaaten Bezüge zu den Zielen der EU für 2025 und 2030 enthalten. Außerdem wurde der europäische Kodex für die elektronische Kommunikation in mehreren Ländern noch nicht in nationales Recht umgesetzt und die Vergabe von 5G-Frequenzen hat sich verzögert. Die Verzögerungen bei der Frequenzvergabe haben unterschiedliche Gründe: eine schwache Nachfrage seitens der Mobilfunknetzbetreiber, Probleme bei der grenzüberschreitenden Koordinierung mit Nicht-EU-Ländern entlang der östlichen Grenzen, die Auswirkungen auf die Auktionszeitpläne aufgrund der COVID-19-Pandemie und die Ungewissheit im Hinblick auf den Umgang mit Sicherheitsfragen. Die Verzögerungen bei der Einführung von 5G in den Mitgliedstaaten sind so groß, dass sie die Verwirklichung der Ziele gefährden. Die Kommission hat die Mitgliedstaaten bei der Umsetzung des 5G-Aktionsplans 2016 durch Hard-Law- und Soft-Law-Initiativen, Leitlinien und die 5G Forschungsfinanzierung unterstützt. Sie hat jedoch die erwartete Qualität der 5G-Dienste nicht klar definiert.

VII Im EU-Instrumentarium für die 5G-Cybersicherheit sind verschiedene strategische, technische und Unterstützungsmaßnahmen zur Bewältigung von Bedrohungen für die 5G-Netzsicherheit aufgeführt, wobei für jede dieser Maßnahmen die zuständigen Akteure benannt werden. Mit einigen dieser Maßnahmen soll dem Problem begegnet werden, dass manche Anbieter von 5G-Ausrüstungen ein hohes Risiko aufweisen. Dieses Instrumentarium wurde von der Kommission und dem Europäischen Rat gebilligt. Die in dem Instrumentarium festgelegten Kriterien bieten einen operativen Rahmen, der für die koordinierte Bewertung des Risikoprofils der Anbieter in allen Mitgliedstaaten hilfreich ist. Gleichzeitig sind für die Durchführung dieser Bewertung nach wie vor die Mitgliedstaaten zuständig. Das Instrumentarium wurde zwar in einer frühen Phase der 5G-Einführung angenommen, aber eine Reihe von Mobilfunknetzbetreibern hatte ihre Anbieter bereits ausgewählt. Seit der Annahme des Instrumentariums wurden bei der Erhöhung der Sicherheit von 5G-Netzen Fortschritte erzielt, wobei die meisten Mitgliedstaaten Hochrisikoanbietern Beschränkungen auferlegt haben oder dabei sind, dies zu tun. In den kommenden Jahren könnten die Gesetze zur 5G-Sicherheit, die von den Mitgliedstaaten auf der Grundlage des Instrumentariums erlassen werden, zu einheitlicheren Ansätzen gegenüber 5G-Hochrisikoanbietern führen. Da jedoch keine der vorgeschlagenen Maßnahmen rechtsverbindlich ist, ist die Kommission nicht befugt, sie durchzusetzen. Daher besteht weiterhin die Gefahr, dass das Instrumentarium als solches nicht

gewährleisten kann, dass die Mitgliedstaaten in Fragen der Netzsicherheit in abgestimmter Weise vorgehen.

VIII Die Kommission hat das Problem sicherheitsrelevanter ausländischer Subventionen für 5G-Anbieter in Angriff genommen. Was den Umgang mit möglichen Substitutionskosten durch die Mitgliedstaaten angeht, die entstehen könnten, wenn Mobilfunknetzbetreiber Ausrüstung von Hochrisikoanbietern ohne Übergangszeit aus den EU-Netzen entfernen müssen, mangelt es der Kommission an ausreichenden Informationen.

IX Der Hof empfiehlt der Kommission,

- die gleichmäßige und zügige Einführung von 5G-Netzen in der EU zu fördern;
- ein abgestimmtes Vorgehen der Mitgliedstaaten in Bezug auf die 5G-Sicherheit zu unterstützen;
- die 5G-Sicherheitskonzepte der Mitgliedstaaten zu überwachen und die Auswirkungen von Divergenzen auf das wirksame Funktionieren des Binnenmarkts zu bewerten.

Einleitung

Eigenschaften und Bedeutung von 5G

01 Die "fünfte Generation" von Telekommunikationssystemen, kurz 5G, ist ein neuer globaler Funkstandard. Er zeichnet sich gegenüber 3G- und 4G-Netzen durch eine deutlich höhere Datenkapazität und Übertragungsgeschwindigkeit aus. Zwar enthält 5G einige Netzelemente, die auf früheren Generationen von Mobilfunk- und Drahtlostechnologien basieren, es handelt sich jedoch nicht um eine schrittweise Weiterentwicklung dieser Netze. Der neue Funkstandard ermöglicht eine universelle Konnektivität mit ultrahoher Bandbreite und geringer Latenz für Einzelnutzer und verbundene Geräte.

02 Über 5G werden mehr Geräte als je zuvor im "Internet der Dinge" miteinander verbunden sein. Ende 2018 waren weltweit schätzungsweise 22 Milliarden Geräte mit Netzanbindung im Einsatz. Prognosen zufolge dürfte sich diese Zahl bis 2030 auf etwa 50 Milliarden erhöhen[1] und zur Entstehung eines riesigen Netzes miteinander verbundener Geräte, von Smartphones bis hin zu Küchengeräten, führen. Es wird erwartet, dass der weltweite Datenverbrauch von 12 Exabyte pro Monat im Jahr 2017[2] auf über 5 000 Exabyte bis 2030[3] ansteigen wird.

03 5G-Dienste sind eine wesentliche Voraussetzung für ein breites Spektrum an innovativen Anwendungen mit dem Potenzial, viele Bereiche der EU-Wirtschaft zu verändern und den Alltag der Bürgerinnen und Bürger zu verbessern (siehe ***Abbildung 1***). Eine im Auftrag der Kommission durchgeführte Studie aus dem Jahr 2017 ergab, dass sich der Nutzen der Einführung von 5G in vier wichtigen strategischen Industriezweigen (Automobilindustrie, Gesundheit, Verkehr und Energie) auf bis zu 113 Milliarden Euro pro Jahr belaufen könnte[4]. Außerdem wird darin prognostiziert, dass im Zuge der Einführung von 5G 2,3 Millionen Arbeitsplätze in den Mitgliedstaaten

---

[1] Statista, Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030.

[2] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017-2022, Februar 2019.

[3] ITU-R, IMT traffic estimates for the years 2020 to 2030.

[4] Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, Februar 2017.

geschaffen werden. Einer Studie aus dem Jahr 2021 zufolge wird das europäische Bruttoinlandsprodukt (BIP) durch 5G zwischen 2021 und 2025 schätzungsweise um bis zu 1 Billion Euro wachsen. Infolgedessen könnten bis zu 20 Millionen Arbeitsplätze in sämtlichen Wirtschaftsbereichen neu geschaffen oder umgewandelt werden[5].

Abbildung 1 – 5G wird alle Aspekte unseres Lebens abdecken

Quelle: Europäische Kommission.

Sicherheitsbedenken

04 5G bietet viele Wachstumschancen, birgt aber auch Risiken (siehe ***Anhang I*** zu den wichtigsten Chancen und Risiken von 5G). Ein solches Risiko sind Sicherheitsbedrohungen. Telekommunikationssysteme waren schon immer durch Cyberangriffe gefährdet (siehe ***Anhang II***)[6]. Von besonderer Bedeutung sind Sicherheitsaspekte bei 5G deshalb, weil 5G wegen der zugrunde liegenden Technologie und insbesondere aufgrund seiner Abhängigkeit von Software eine größere Angriffsfläche bietet als 3G- oder 4G-Telekommunikationssysteme[7].

---

[5] Accenture Strategy, The Impact of 5G on the European Economy, Februar 2021.

[6] Analyse Nr. 02/2019: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU (Themenpapier), Kontaktausschuss der obersten Rechnungskontrollbehörden 2020, Prüfungskompendium – Cybersicherheit und Wissenschaftlicher Dienst des Europäischen Parlaments – Europäisches Wissenschaftsmedienzentrum.

[7] NIS-Kooperationsgruppe, EU coordinated risk assessment of the cybersecurity of 5G networks, 9.10.2019. Punkt 3.4.

05 Da 5G-Netze voraussichtlich das Rückgrat vielfältiger Dienste und Anwendungen bilden werden, wird die Verfügbarkeit dieser Netze zu einer großen Herausforderung für die nationale und die europäische Sicherheit. Sollten Hacker in ein 5G-Netz eindringen, könnten sie in dessen Kernfunktionen eingreifen, um Dienste zu unterbrechen oder die Kontrolle über kritische Infrastrukturen (z. B. Stromnetze) zu übernehmen, die in der EU häufig grenzübergreifend ausgelegt sind. In Studien werden die weltweiten wirtschaftlichen Auswirkungen der Cyberkriminalität auf bis zu 5 000 Milliarden Euro pro Jahr veranschlagt, das entspricht mehr als 6 % des weltweiten BIP im Jahr 2020[8].

06 Eine weitere Herausforderung für die 5G-Sicherheit ist die entscheidende Rolle, die einigen wenigen Anbietern beim Aufbau und Betrieb von 5G-Netzen zukommt. So erhöht sich das Risiko einer möglichen Versorgungsunterbrechung, wenn eine Abhängigkeit von einem einzigen Anbieter besteht – insbesondere wenn dieser Anbieter ein hohes Risiko birgt, z. B. wenn er Eingriffen vonseiten eines Nicht-EU-Staates unterliegt. Im Jahr 2019 wies die mit Vertretern der Mitgliedstaaten und der EU-Einrichtungen besetzte Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe) darauf hin, dass "feindlich gesinnte staatliche Akteure" über einen privilegierten Zugang, durch Druck auf einen Anbieter oder unter Berufung auf nationale Rechtsvorschriften auf einfache Weise Zugang zu einem 5G-Netz erhalten könnten[9] (siehe ***Kasten 1***). Vor diesem Hintergrund begann die EU mit der Entwicklung von Initiativen zur Verbesserung der 5G-Sicherheit.

Kasten 1

Sicherheitsbedenken im Kontext der Zusammenarbeit zwischen der EU und China im Bereich 5G

- Im Jahr 2015 unterzeichnete die EU eine gemeinsame Erklärung mit China zur strategischen Zusammenarbeit im Bereich 5G, in der sie sich zu Gegenseitigkeit und Offenheit in Bezug auf den Zugang zur Forschungsförderung für 5G-Netze und den Marktzugang verpflichtete[10].

---

[8] Weltwirtschaftsforum, Wild Wide Web – Consequences of Digital Fragmentation, 2021.

[9] NIS-Kooperationsgruppe, EU coordinated risk assessment of the cybersecurity of 5G networks, 9.10.2019.

[10] https://ec.europa.eu/commission/presscorner/detail/de/IP_15_5715

- Im Jahr 2017 verabschiedete China ein Nachrichtendienstgesetz, demzufolge alle chinesischen Organisationen sowie die Bürgerinnen und Bürger Chinas mit dem nationalen Nachrichtendienst zusammenarbeiten und Stillschweigen darüber bewahren müssen[11]. Als Reaktion darauf haben die USA im Jahr 2018 Maßnahmen ergriffen, um die Geschäftstätigkeit mehrerer chinesischer Unternehmen – darunter Huawei, einem wichtigen 5G-Anbieter – einzuschränken.

Im März 2019 äußerte auch das Europäische Parlament die Sorge, dass chinesische 5G-Anbieter aufgrund der Gesetze ihres Herkunftslands ein Sicherheitsrisiko für die EU darstellen könnten.

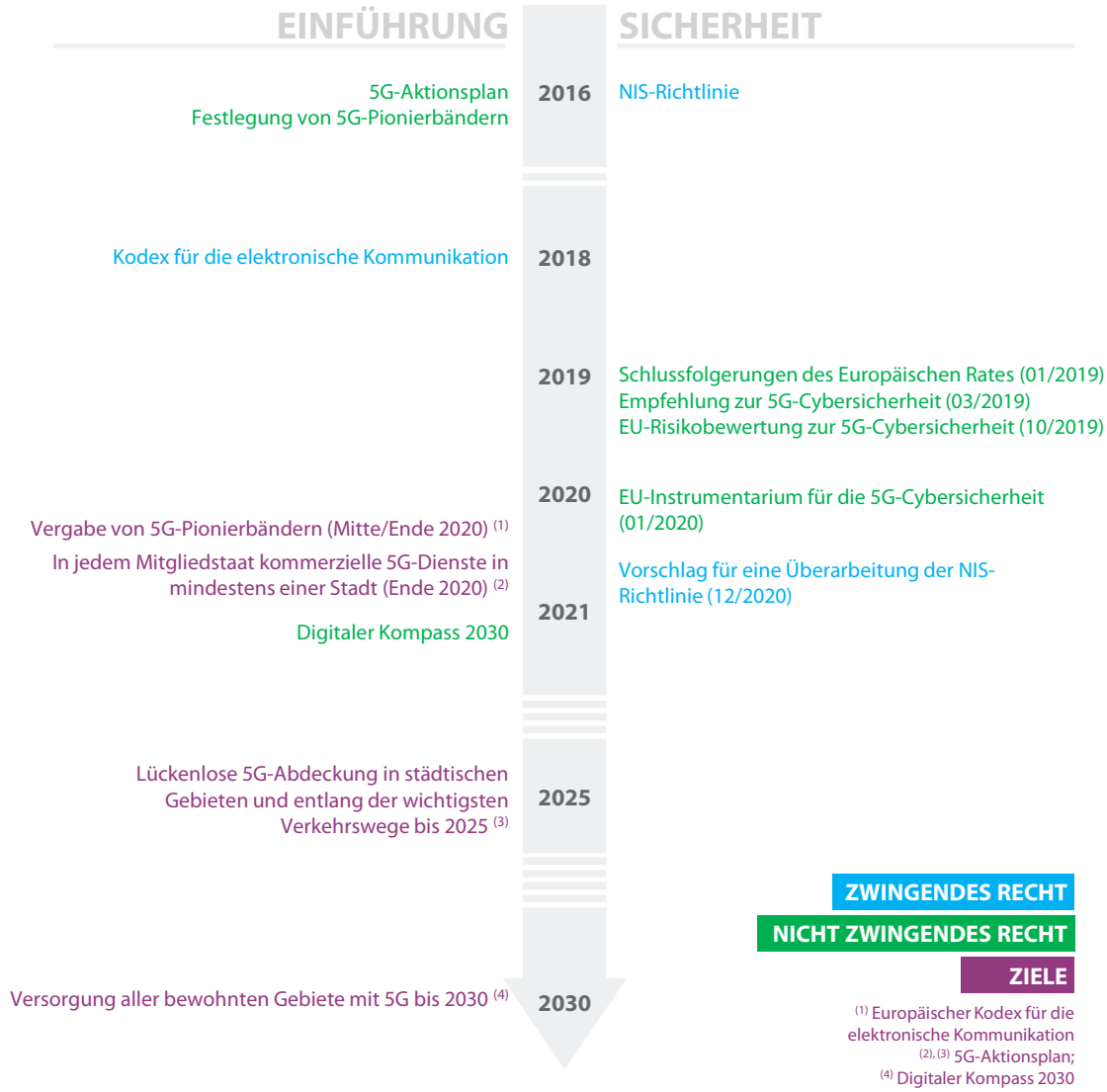
07 Vertraulichkeit und Privatsphäre sind ebenfalls potenziell bedroht, da Telekommunikationsbetreiber ihre Daten oft an Rechenzentren auslagern. Es besteht die Gefahr, dass diese Daten auf Ausrüstung von 5G-Anbietern gespeichert werden, die in Nicht-EU-Ländern mit einem anderen Rechts- und Datenschutzniveau als in der EU ansässig sind.

5G-Initiativen auf EU-Ebene

08 Der politische Rahmen für 5G und die 5G-Sicherheit besteht sowohl aus sogenanntem *Hard Law*, d. h. "zwingendem Recht", das rechtlich bindend und durchsetzbar ist (z. B. Verordnungen), als auch aus *Soft Law*, d. h. "nicht zwingendem" Recht (z. B. Mitteilungen der Kommission). In ***Anhang III*** wird der rechtliche und politische Rahmen beschrieben. Aus ***Abbildung 2*** sind die wichtigsten Politikdokumente sowie die Hauptziele zu ersehen.

[11] Entschließung des Europäischen Parlaments vom 12. März 2019; Nachrichtendienstgesetz der Volksrepublik China, Artikel 14. Siehe auch Übersetzung unter https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

Abbildung 2 – Die wichtigsten Politikdokumente und die Hauptziele hinsichtlich der Einführung und der Sicherheit von 5G



Quelle: Europäischer Rechnungshof.

Aufgaben und Zuständigkeiten

09 Während die Mobilfunknetzbetreiber für die sichere Einführung von 5G unter Einsatz der Ausrüstung von Technologieanbietern verantwortlich sind und die nationale Sicherheit in die Zuständigkeit der Mitgliedstaaten fällt, ist die Sicherheit der 5G-Netze jedoch ein Thema, das für den gesamten Binnenmarkt und die technologische Souveränität der EU von strategischer Bedeutung ist[12]. Hinsichtlich der technischen und sicherheitsrelevanten Aspekte der 5G-Netze unterstützen und

[12] https://ec.europa.eu/commission/presscorner/detail/de/IP_20_12

koordinieren die Kommission und die EU-Agenturen daher die Maßnahmen der Mitgliedstaaten.

10 In ***Tabelle 1*** werden die wichtigsten Aufgaben und Zuständigkeiten bei 5G-Netzen näher erläutert.

Tabelle 1 – Aufgaben und Zuständigkeiten

	Kommission und EU-Agenturen	Behörden der Mitgliedstaaten	Mobilfunknetzbetreiber und 5G-Anbieter
Bereitstellung und Zuteilung von 5G-Pionierbändern		✓	
Festlegung der 5G-Politik der EU	✓	✓	
Einführung von 5G-Netzen			✓
Investitionen und Finanzierung	✓	✓	✓
Nationale Sicherheit		✓	
Sicherheit der 5G-Netze		✓	✓
Unterstützung und Koordinierung von Maßnahmen der Mitgliedstaaten	✓		

Quelle: Europäischer Rechnungshof.

Kosten der 5G-Einführung und damit verbundene finanzielle Unterstützung durch die EU

Die Gesamtkosten der 5G-Einführung in allen Mitgliedstaaten könnten sich auf bis zu 400 Milliarden Euro belaufen

11 Im Jahr 2021 wurde geschätzt, dass die Gesamtkosten für die 5G-Einführung in allen EU-Mitgliedstaaten bis 2025 zwischen 281 Milliarden und 391 Milliarden Euro belaufen werden; sie werden hälftig auf die Schaffung einer neuen 5G-Infrastruktur und die Ertüchtigung der vorhandenen Festnetzinfrastruktur für Gigabit-Geschwindigkeiten entfallen[13]. Zum größten Teil müssen diese Investitionen von den Mobilfunknetzbetreibern finanziert werden.

[13] Schätzung der Kommission auf der Grundlage von Daten von EIB, Analysys, GSMA und Unternehmensankündigungen sowie ETNO – European Telecommunications, Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All, März 2021.

Im Zeitraum 2014-2020 hat die EU die Entwicklung von 5G mit über vier Milliarden Euro finanziert

12 Im Zeitraum 2014-2020 unterstützte die EU die 5G-Entwicklung mit mehr als vier Milliarden Euro sowohl unmittelbar aus dem EU-Haushalt als auch über Finanzierungen durch die Europäische Investitionsbank (EIB). Aus dem EU-Haushalt wurden Projekte finanziert, die ausschließlich Forschung zum Gegenstand hatten, während die EIB sowohl Forschung als auch Einführung unterstützte.

13 Der größte Teil der EU-Mittel zur Finanzierung von Projekten im Zusammenhang mit 5G wird von der EIB bereitgestellt. Bis August 2021 hat sie für neun 5G-Projekte in fünf Mitgliedstaaten Darlehen in Höhe von insgesamt 2,5 Milliarden Euro gewährt[14]. Darüber hinaus wurden für den Zeitraum 2014-2020 rund 1,9 Milliarden Euro aus dem EU-Haushalt bereitgestellt. ***Tabelle 2*** bietet einen Überblick über die wichtigsten EU-Finanzierungsquellen zur Förderung von 5G.

Tabelle 2 – EU-Finanzmittel für 5G (2014-2020)

EU-Finanzierungsquellen	Betrag
EIB	2,485 Milliarden Euro[1]
Europäischer Fonds für strategische Investitionen (EFSI)	1 Milliarde Euro[2]
Horizont 2020	755 Millionen Euro[3]
EFRE	Mindestens 147 Millionen Euro[4]

1) EIB-Projektliste.
2) EFSI-Projektliste.
3) Dashboard Horizont 2020.
4) Datensatz der aus dem EFRE kofinanzierten Projekte während des mehrjährigen Finanzrahmens 2014-2020.

Quelle: Europäischer Rechnungshof.

14 Aus dem (von der EIB verwalteten) EFSI wurden zwei Projekte zum Ausbau des Funkzellennetzes und zur Verbesserung der Standardisierung gefördert. Insgesamt beliefen sich die Investitionskosten dieser Projekte auf 3,9 Milliarden Euro, darunter 1 Milliarde Euro aus dem EFSI (siehe ***Anhang IV***).

[14] EIB-Projektliste.

15 Seit 2014 hat die Kommission außerdem mehr als 100 5G-Projekte mit Mitteln aus Horizont 2020 – und in geringerem Umfang aus dem EFRE – direkt kofinanziert. ***Anhang V*** enthält Beispiele solcher Projekte.

Aus der Aufbau- und Resilienzfazilität werden in den kommenden Jahren zusätzliche EU-Mittel für die 5G-Einführung bereitgestellt

16 Die Aufbau- und Resilienzfazilität wird in den kommenden Jahren eine zusätzliche Finanzierungsquelle für die Einführung von 5G sein. Bis September 2021 hatten 16 Mitgliedstaaten die Finanzierung der 5G-Einführung über die Aufbau- und Resilienzfazilität geplant, 10 entschieden sich dagegen. Aus einem Mitgliedstaat lagen noch keine Informationen vor.

Prüfungsumfang und Prüfungsansatz

17 Im Rahmen dieser Prüfung hat der Hof untersucht, ob die Kommission die Mitgliedstaaten wirksam dabei unterstützt,

- die EU-Ziele für 2025 und 2030 für die Einführung und den Ausbau ihrer 5G-Netze zu erreichen;
- sich in abgestimmter Weise mit Sicherheitsbedenken hinsichtlich 5G auseinanderzusetzen.

In beiden Bereichen untersuchte der Hof außerdem die Maßnahmen und Tätigkeiten der Mitgliedstaaten.

18 Als "5G-Sicherheit" bezeichnet der Hof sowohl die Cybersicherheit als auch die Sicherheit der Hard- und Software. Der Hof untersuchte sowohl die Sicherheit als auch die Einrichtung von 5G-Netzen, für die das Jahr 2020 von zentraler Bedeutung war (siehe ***Abbildung 2***). Mit seinem Bericht möchte der Hof Erkenntnisse und Empfehlungen für die zügige Einführung sicherer 5G-Netze in der EU bereitstellen.

19 Die Prüfung durch den Hof erstreckte sich auf den Zeitraum zwischen 2016 und Mai 2021. Soweit möglich berücksichtigte der Hof weitere aktuelle Informationen. Der Hof führte folgende Prüfungshandlungen durch:

- Überprüfung von EU-Rechtsvorschriften, Kommissionsinitiativen und anderen einschlägigen Unterlagen;
- Befragung von Vertretern der Kommission, der EIB, des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie von Telekommunikationsverbänden, Mobilfunknetzbetreibern, 5G-Anbietern, internationalen Organisationen und einschlägigen Experten und Behörden in Finnland, Deutschland, Polen und Spanien, um Erkenntnisse zu gewinnen. Die Auswahl der Mitgliedstaaten erfolgte anhand verschiedener Kriterien (u. a. Höhe der bereitgestellten EU-Mittel für 5G-Projekte, Stand der Einführung und geografische Ausgewogenheit);
- Befragung aller 27 für den Telekommunikationsbereich zuständigen nationalen Regulierungsbehörden in der EU, um einen umfassenderen Überblick über die mit 5G verbundenen Herausforderungen in den Mitgliedstaaten zu erhalten;

- Überprüfung von 10 von der EU (aus dem EFSI, dem EFRE und Horizont 2020) kofinanzierten Beispielprojekten im Bereich 5G.

20 Außerdem stützte sich der Hof auf seine jüngste Analyse der Reaktion der EU auf Chinas staatlich gelenkte Investitionsstrategie[15] sowie auf weitere Berichte, z. B. über den Breitbandausbau[16], die Initiative "Digitalisierung der europäischen Industrie"[17] und die Cybersicherheitspolitik der EU[18].

[15] Analyse Nr. 03/2020 "Die Reaktion der EU auf Chinas staatlich gelenkte Investitionsstrategie".

[16] Sonderbericht Nr. 12/2018 "Der Breitbandausbau in den EU-Mitgliedstaaten: Trotz Fortschritten werden nicht alle Ziele der Strategie Europa 2020 erreicht".

[17] Sonderbericht Nr. 19/2020 "Digitalisierung der europäischen Industrie: ehrgeizige Initiative, deren Erfolg vom dauerhaften Engagement der EU, der Regierungen und der Unternehmen abhängt".

[18] Analyse Nr. 02/2019 "Herausforderungen für eine wirksame Cybersicherheitspolitik der EU (Themenpapier)".

Feststellungen

Verzögerungen bei der Einführung von 5G-Netzen gefährden die Erreichung der EU-Ziele für 2025 und 2030

21 Mit Blick auf die zügige Einführung von 5G-Netzen untersuchte der Hof, ob

- die Mitgliedstaaten bei der Einführung von 5G im Zeitplan liegen;
- die Kommission die Mitgliedstaaten angemessen unterstützt hat;
- die Mitgliedstaaten wesentliche Hindernisse für den raschen Ausbau der 5G-Netze beseitigt haben.

Die Mitgliedstaaten liegen bei der 5G-Einführung hinter dem Zeitplan

Die Kommission hat in ihrem 5G-Aktionsplan von 2016 Fristen für die Einführung von 5G-Netzen festgelegt

22 In ihrem 5G-Aktionsplan von 2016 hat die Kommission Fristen für die Einführung von 5G-Netzen in der EU vorgeschlagen: Die Mitgliedstaaten sollten die ersten 5G-Netze bis Ende 2018 einführen, bis Ende 2020 in mindestens einer Großstadt kommerzielle 5G-Dienste anbieten und bis 2025 eine lückenlose 5G-Abdeckung in städtischen Gebieten und entlang wichtiger Verkehrswege sicherstellen.

23 Im März 2021 gab die Kommission als weiteres Ziel die 5G-Abdeckung aller besiedelten Gebiete bis 2030 vor[19].

Bis Ende 2020 hatten 23 Mitgliedstaaten kommerzielle 5G-Dienste eingeführt

24 Bis Ende 2020 hatten 23 Mitgliedstaaten das Ziel erreicht, dass mindestens eine Großstadt über Zugang zu 5G-Diensten verfügt. Nur in Zypern, Litauen, Malta und Portugal wurde dieses Ziel verfehlt. Ende Oktober 2021 boten nur Litauen und Portugal noch keine 5G-Dienste in ihren Städten an.

---

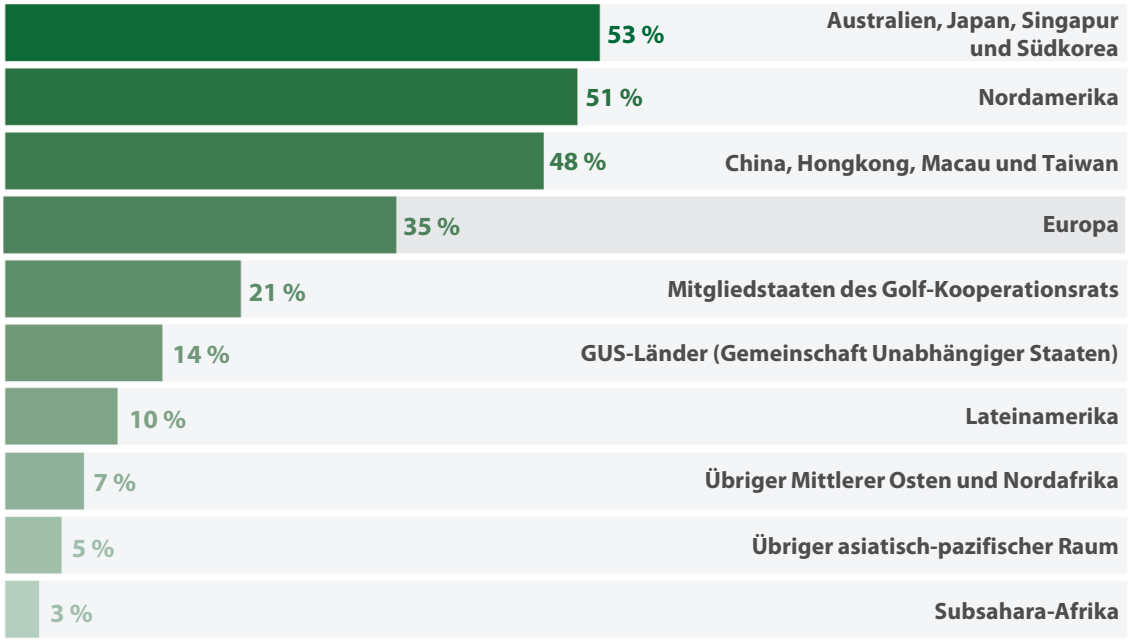
[19] Europäische Kommission, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade, COM(2021) 118 final.

Es besteht die Gefahr, dass die meisten Mitgliedstaaten die Fristen 2025 und 2030 nicht einhalten werden

25 Laut einer aktuellen Studie der Kommission werden voraussichtlich nur 11 Mitgliedstaaten bis 2025 eine lückenlose 5G-Abdeckung in allen städtischen Gebieten sowie entlang der wichtigsten Landverkehrswege erreichen[20]. Für die übrigen 16 Mitgliedstaaten schätzt die Kommission die Wahrscheinlichkeit, dieses Ziel zu erreichen, entweder als mittel (Deutschland, Estland, Irland, Litauen, Österreich, Polen, Slowenien und Tschechien) oder gering (Belgien, Bulgarien, Griechenland, Kroatien und Zypern) ein.

26 Im Jahr 2021 stellte der Industrieverband *Global System for Mobile Communications Association* (GSMA) fest, dass die Einführung von 5G in der EU im Vergleich zu anderen Teilen der Welt unterschiedlich schnell voranschreitet. Beispielsweise wird Schätzungen zufolge der Anteil der 5G-basierten Mobilfunkverbindungen in Nordamerika bis 2025 51 % aller Mobilfunkverbindungen betragen, während ihr Anteil in Europa (einschließlich Nicht-EU-Länder) bei lediglich 35 % liegen wird (siehe ***Abbildung 3***).

Abbildung 3 – Anteil der 5G-Verbindungen an allen Mobilfunkverbindungen bis 2025



Quelle: GSMA. The Mobile Economy 2021.

[20] Study on National Broadband Plans in the EU-27.

27 Angesichts des derzeitigen Tempos der Einführung besteht ein hohes Risiko, dass die meisten Mitgliedstaaten die Frist 2025 − und damit auch die Frist 2030 für die Abdeckung aller besiedelten Gebiete − nicht einhalten werden. Vor diesem Hintergrund untersuchte der Hof, ob die Kommission die Mitgliedstaaten wirksam dabei unterstützt hat, die 5G-Ziele der EU für 2025 und 2030 für die Einführung und den Ausbau ihrer 5G-Netze zu erreichen.

Einige Mängel bei der Unterstützung der Mitgliedstaaten durch die Kommission

Die Kommission hat die erwartete Dienstqualität von 5G-Netzen nicht definiert

28 Bislang hat die Kommission die erwartete Dienstqualität von 5G-Netzen, insbesondere in Bezug auf Mindestgeschwindigkeit und maximale Latenz, nicht definiert. Außerdem wurden die Mitgliedstaaten im Aktionsplan 2016 aufgefordert, bis Ende 2020 "rein privatwirtschaftliche" 5G-Dienste in Europa einzuführen, ohne diese qualitätsbezogenen Konzepte jedoch zu definieren.

29 Der Mangel an Klarheit hinsichtlich der erwarteten Dienstqualität birgt die Gefahr, dass diese Begriffe von den Mitgliedstaaten unterschiedlich ausgelegt werden. Der Hof stellte Beispiele für unterschiedliche Ansätze bei der Einführung von 5G in den einzelnen Mitgliedstaaten fest (siehe ***Kasten 2***).

Kasten 2

Beispiele für unterschiedliche Ansätze bei der Einführung von 5G

Geschwindigkeit und Latenz sind zwei Schlüsselaspekte der Leistung 5G-basierter Dienste. Beispielsweise erfordern die 5G-basierte Tele-Chirurgie oder die industrielle Automatisierung sehr hohe Geschwindigkeiten und geringe Latenzzeiten. Bislang haben jedoch nur zwei Mitgliedstaaten (Deutschland und Griechenland) Festlegungen für die Mindestgeschwindigkeit und die maximale Latenz getroffen[21].

[21] 5G Observatory Quarterly Report 12, bis Juni 2021.

Die Forderung, dass mindestens eine Großstadt bis Ende 2020 Zugang zu 5G-Diensten haben sollte, wurde von den Mitgliedstaaten unterschiedlich ausgelegt. Daher kann das Spektrum der Städte, in denen 5G-Dienste verfügbar sind, von Städten mit nur wenigen abgedeckten Straßen (z. B. in Luxemburg) bis zu Städten mit nahezu flächendeckender Abdeckung (z. B. Helsinki) reichen. ***Anhang VI*** enthält Angaben zur Abdeckung in ausgewählten Städten.

30 Sollte diese Situation fortbestehen, könnte es zu Ungleichheiten beim Zugang zu 5G-Diensten und deren Qualität in der EU kommen ("digitale Kluft"), d. h. in einem Teil der EU hätten die Bürgerinnen und Bürger einen besseren Zugang zu 5G-Diensten und zu einer besseren Dienstqualität als im Rest der EU. Diese digitale Kluft könnte sich auch auf das Potenzial der wirtschaftlichen Entwicklung auswirken, da Sektoren wie das Gesundheitswesen, das Bildungswesen und der Arbeitsmarkt nur dann eine grundlegende Umgestaltung durch 5G erfahren können, wenn 5G mit einer ausreichenden Leistung verfügbar ist.

31 Klarheit über die erwartete Leistung der 5G-Netze ist auch in Bezug auf die Initiative der Kommission erforderlich, die eine größere Transparenz hinsichtlich der Dienstqualität der Mobilfunknetzbetreiber beim Roaming vorsieht und für die die Kommission kürzlich einen Legislativvorschlag vorgelegt hat[22].

Die vierteljährliche Berichterstattung der Kommission über den 5G-Ausbau ist nicht immer zuverlässig

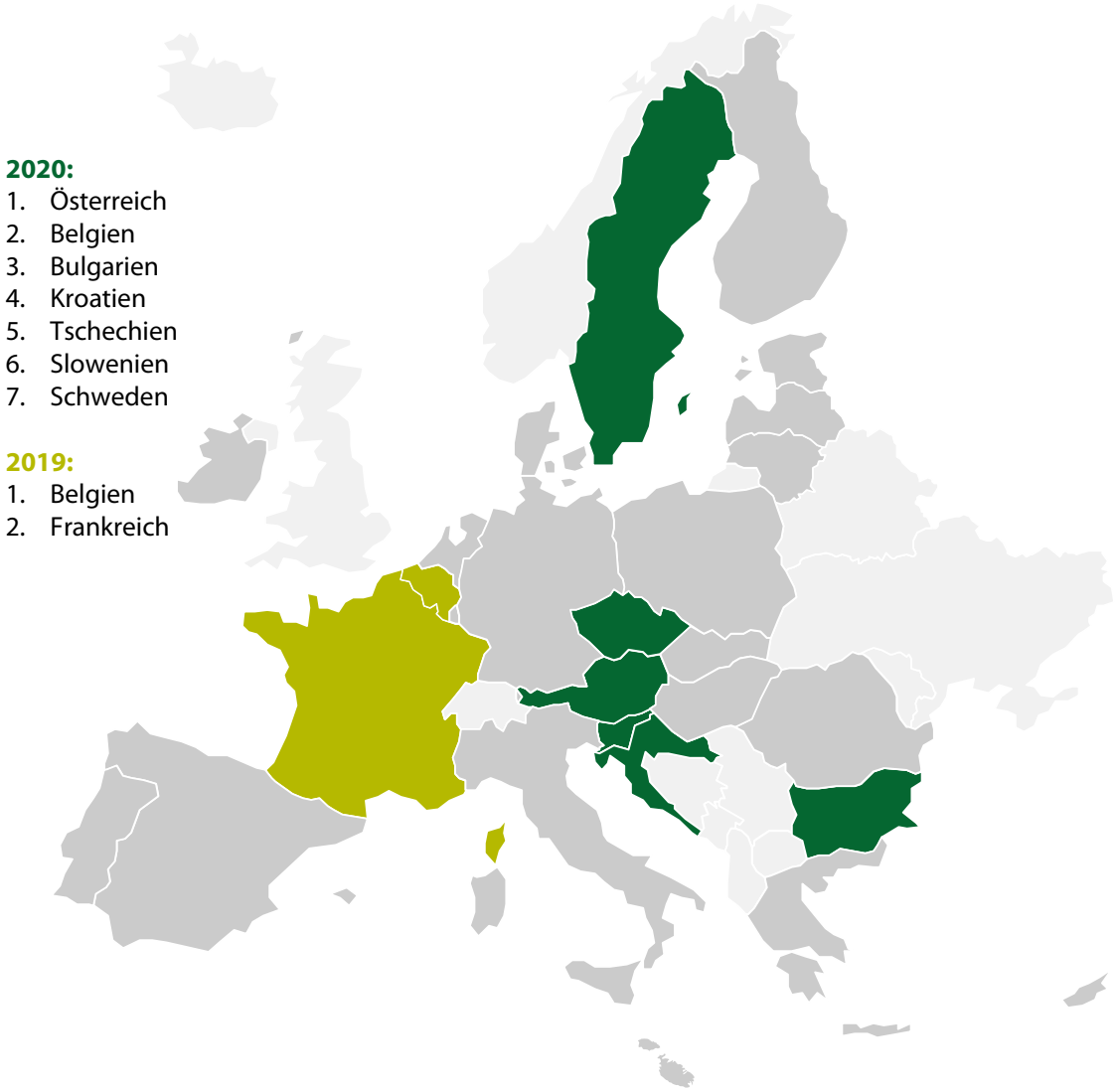
32 Über die 5G-Beobachtungsstelle überwacht die Kommission den Stand der 5G-Einführung in den Mitgliedstaaten. Diese Beobachtungsstelle liefert vierteljährlich Informationen über die 5G-Einführung und die 5G-Strategien der Mitgliedstaaten. Der Hof stellte jedoch fest, dass die in diesen Berichten enthaltenen Informationen in zwei der vier überprüften Länder nicht immer zuverlässig waren. Im Quartalsbericht Nr. 10 mit Informationen bis Ende Dezember 2020 beispielsweise wurde die Zahl der finnischen Gemeinden, die über 5G verfügen, deutlich zu niedrig angegeben (40 statt 70) und es fehlte die Angabe, dass die Versteigerung von 5G-Frequenzen in Polen verschoben wurde (siehe Ziffer ***42***).

[22] Europäische Kommission, Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über das Roaming in öffentlichen Mobilfunknetzen in der Union (Neufassung), COM(2021) 85 final vom 24.2.2021.

Eine Überwachung der Fortschritte der Mitgliedstaaten bei der Einführung von 5G-Netzen durch die Kommission ist erst in letzter Zeit im Rahmen des Europäischen Semesters erfolgt

33 Der Hof stellte fest, dass die Kommission in den letzten beiden Jahren mehr Anstrengungen im Rahmen des Europäischen Semesters unternommen hat, um Fortschritte der Mitgliedstaaten bei der Einführung von 5G-Netzen zu unterstützen. Die Anzahl der länderspezifischen Empfehlungen mit direktem Bezug zu 5G hat sich von zwei Mitgliedstaaten im Jahr 2019 auf sieben Mitgliedstaaten im Jahr 2020 erhöht (siehe ***Abbildung 4***).

Abbildung 4 – Länderspezifische Empfehlungen zu 5G



Quelle: Europäischer Rechnungshof, auf der Grundlage länderspezifischer Empfehlungen.

Die Mitgliedstaaten müssen noch wesentliche Hindernisse für einen zügigen Ausbau der 5G-Netze beseitigen

34 Um die EU-Ziele für die Einführung von 5G in den Jahren 2025 und 2030 zu erreichen, müssen die Mitgliedstaaten drei wichtige Grundvoraussetzungen erfüllen: in strategischer Hinsicht gilt es sicherzustellen, dass ihre nationalen 5G-Strategien oder -Breitbandpläne diese Ziele widerspiegeln[23], auf legislativem Gebiet ist der Europäische Kodex für die elektronische Kommunikation (*European Electronic Communications Code*, EECC) von 2018 umzusetzen[24], und wirtschaftlich gesehen ist die Zuweisung von Funkfrequenzen zu vollziehen[25]. ***Tabelle 3*** enthält eine Übersicht über die Fortschritte der Mitgliedstaaten im Hinblick auf diese drei Voraussetzungen.

[23] Studie der Kommission zu nationalen Breitbandplänen in der EU-27.

[24] Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

[25] Mitteilung der Europäischen Kommission, Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums, COM(2020) 50 final.

Tabelle 3 – Aktueller Stand hinsichtlich der Erfüllung der Voraussetzungen für die Erreichung der Ziele für 2025

Mitgliedstaat	NBP gemäß den Zielen für 2025	Umsetzung der EECC-Richtlinie	5G-Pionierbänder (August 2021)			Wahrscheinlichkeit der Erreichung des Ziels
			700 MHz	3,6 GHz	26 GHz	
Belgien				Vorläufige Nutzung		gering
Bulgarien		✓		✓		gering
Tschechien	✓	✓	✓	✓		mittel
Dänemark		✓	✓	✓	✓	hoch
Deutschland	✓	✓	✓	✓	✓	mittel
Estland						mittel
Irland				✓		mittel
Griechenland	✓	✓	✓	✓	✓	gering
Spanien	✓		✓	✓		hoch
Frankreich	✓	✓	✓	✓		hoch
Kroatien			✓	✓	✓	gering
Italien			✓	✓	✓	hoch
Zypern	✓		✓	✓		gering
Litauen	✓					mittel
Lettland				✓		hoch
Luxemburg			✓	✓		hoch
Ungarn	✓	✓	✓	✓		hoch
Malta		✓				mittel
Niederlande	✓		✓			mittel
Österreich	✓	✓	✓	✓		mittel
Polen	✓					mittel
Portugal				Vorläufige Nutzung		mittel-hoch
Rumänien						hoch
Slowenien	✓		✓	✓	✓	mittel
Slowakei			✓			hoch
Finnland	✓	✓	✓	✓	✓	hoch
Schweden	✓		✓	✓		hoch

Quelle: Study on National Broadband Plans in the EU-27, Kommission, 5G-Beobachtungsstelle und Gruppe für Frequenzpolitik.

Nur wenige Mitgliedstaaten haben die für die Jahre 2025 und 2030 festgelegten Einführungsziele in ihre nationalen 5G-Strategien aufgenommen

35 Die Mitgliedstaaten legen ihre 5G-Politik fest, indem sie spezielle nationale 5G-Strategien erarbeiten oder ihre bestehenden nationalen Breitbandpläne aktualisieren. In der Studie der Kommission zu den nationalen Breitbandplänen aus dem Jahr 2021[26] wird festgestellt, dass nur 14 Mitgliedstaaten das Ziel der EU, bis 2025 eine ununterbrochene 5G-Abdeckung für alle städtischen Gebiete und wichtigen Landverkehrswege zu erreichen, in ihre nationalen 5G-Strategien oder die aktualisierten nationalen Breitbandpläne aufgenommen haben (siehe ***Tabelle 3***). Die Einbeziehung dieses Ziels ist jedoch der Schlüssel zur erfolgreichen Umsetzung der Politik.

Die meisten Mitgliedstaaten haben die EECC-Richtlinie bis Ende 2020 nicht umgesetzt

36 Die Richtlinie über den europäischen Kodex für die elektronische Kommunikation, in der die Aufgaben der nationalen Regulierungsbehörden und die Fristen für die Zuweisung von 5G-Pionierbändern festgelegt sind, hätte von den Mitgliedstaaten bis zum 21. Dezember 2020 umgesetzt werden müssen. Bis Ende Februar 2021 hatten nur drei Mitgliedstaaten (Finnland, Griechenland und Ungarn) erklärt, alle erforderlichen Maßnahmen zur Umsetzung der Richtlinie ergriffen zu haben. Infolgedessen leitete die Kommission Vertragsverletzungsverfahren gegen die übrigen 24 Mitgliedstaaten ein[27].

37 Ende November 2021 waren 23 Vertragsverletzungsverfahren noch nicht abgeschlossen. Während die Kommission die Vertragsverletzungsverfahren gegen sechs Mitgliedstaaten (Bulgarien, Deutschland, Frankreich, Malta, Österreich und Tschechien) in Kürze einstellen wird, muss die Kommission die Fälle der übrigen 17 Mitgliedstaaten möglicherweise vor den Gerichtshof der Europäischen Union bringen[28] (siehe ***Tabelle 3***).

---

[26] Study on National Broadband Plans in the EU-27.

[27] Pressemitteilung der Kommission IP/21/206 vom 4.2.2021.

[28] Pressemitteilung der Kommission IP/21/4612 vom 23.9.2021.

Die Zuweisung von 5G-Pionierbändern verzögert sich

38 Im Jahr 2016 legten die Kommission und die Mitgliedstaaten drei Pionierbänder fest, die für 5G-Dienste genutzt werden sollen:

- das 700-MHz-Frequenzband, mit dem drahtlose Signale besser in Gebäude eindringen, was den Betreibern ermöglicht, eine breitere Abdeckung (Hunderte von Quadratkilometern) zu gewährleisten. Die Geschwindigkeit und Latenz des 5G-Netzes ist jedoch nur eine Stufe über der von 4G (von 150 auf 250 Megabit pro Sekunde);

- das Mittelbandspektrum bei 3,6 GHz, das erhebliche Datenmengen (bis zu 900 Megabit pro Sekunde) über erhebliche Entfernungen (Radius von mehreren Kilometern) übertragen kann;

- das Hochbandspektrum bei 26 GHz, das schnelle Geschwindigkeiten zwischen 1 und 3 Gigabit pro Sekunde über kurze Entfernungen (d. h. weniger als 2 km), aber mit größerer Interferenzempfindlichkeit ermöglicht.

39 Die Mitgliedstaaten sollten das niederbandige Spektrum bis zum 30. Juni 2020 zur Verfügung stellen[29], das Mittelband- und das Hochbandspektrum sollten bis zum 31. Dezember 2020 folgen[30]. Bis Ende 2020 hatten die Mitgliedstaaten jedoch weniger als 40 % der insgesamt verfügbaren Pionierbänder zugewiesen (siehe ***Tabelle 4***):

- Das 700-MHz-Band wurde in 13 Mitgliedstaaten zugewiesen.

- Das 3,6-GHz-Band wurde in 17 Mitgliedstaaten zugewiesen (darunter zwei Mitgliedstaaten, die eine vorläufige Nutzung gewährt hatten).

- Das 26-GHz-Band wurde in vier Mitgliedstaaten zugewiesen.

Bis Ende Oktober 2021 war die Zuweisungsquote auf 53 % gestiegen[31].

---

[29] Beschluss (EU) 2017/899 über die Nutzung des Frequenzbands 470-790 MHz in der Union.

[30] Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

[31] 5G-Beobachtungsstelle und Gruppe für Frequenzpolitik.

Tabelle 4 – Aktueller Stand der Zuweisung von 5G-Pionierbändern, Dezember 2020

Mitgliedstaat	700 MHZ	3,6 GHZ	26 GHZ
Belgien		Vorläufige Nutzung	
Bulgarien			
Tschechien	✓	✓	
Dänemark	✓	✓	✓
Deutschland	✓	✓	✓
Estland		-	
Irland		✓	
Griechenland	✓	✓	✓
Spanien		✓	
Frankreich	✓	✓	
Kroatien			
Italien		✓	✓
Zypern	✓	✓	
Lettland		✓	
Litauen			
Luxemburg	✓	✓	
Ungarn	✓	✓	
Malta			
Niederlande	✓		
Österreich	✓	✓	
Polen			
Portugal		Vorläufige Nutzung	
Rumänien			
Slowenien			
Slowakei	✓	✓	
Finnland	✓	✓	✓
Schweden	✓	✓	

Quelle: 5G-Beobachtungsstelle und Gruppe für Frequenzpolitik.

40 Der Hof stellte fest, dass die Verzögerungen bei der Zuweisung des 26-GHz-Bands hauptsächlich auf eine schwache Nachfrage seitens der Mobilfunknetzbetreiber zurückzuführen sind. In Spanien beispielsweise stehen aus dem 26-GHz-Band nur insgesamt 1,5 GHz für 5G zur Verfügung. Eine Zuweisung an Betreiber ist allerdings nicht erfolgt, da einer im Juli 2019 abgeschlossenen öffentlichen Konsultation zufolge keine entsprechende Nachfrage besteht. Bis Ende 2021 soll eine weitere öffentliche

Konsultation durchgeführt werden, damit das Frequenzband im zweiten Quartal 2022 versteigert werden kann. Auch Mobilfunknetzbetreiber in Finnland stellten fest, dass noch kein großes Interesse am 26-GHz-Band besteht und auch die wirtschaftliche Begründung fehlt.

41 Probleme bei der grenzübergreifenden Koordinierung mit Nicht-EU-Ländern entlang den östlichen Grenzen (Belarus, Russland und Ukraine) trugen ebenfalls zu Verzögerungen bei der 5G-Frequenzvergabe bei. Gemäß den geltenden internationalen Übereinkommen nutzen diese Nicht-EU-Länder das 700-MHz-Band für Fernsehübertragungen und das 3,6-GHz-Band für militärische Satellitenkommunikationsdienste. Dieser Aspekt betrifft vor allem die baltischen Staaten (Estland, Lettland und Litauen) und Polen. Nach Angaben der Kommission wurden einige Fortschritte in Bezug auf die Ukraine und Belarus erzielt, die das 700-MHz-Band bis Ende 2022 freigeben sollen. Die bilateralen Gespräche mit Russland sind noch nicht weiter vorangekommen. Angesichts dieser Situation haben Estland und Polen eine Ausnahmeregelung hinsichtlich der Fristen für die Zuweisung des 700-MHz-Bands bis Mitte 2022 beantragt.

42 Darüber hinaus wurden in Polen und Spanien während der COVID-19-Pandemie Versteigerungen von 5G-Frequenzen verschoben (siehe ***Kasten 3***).

Kasten 3

Beispiele für pandemiebedingte Verzögerungen bei der Zuweisung von 5G-Frequenzen

- Im März 2020 kündigte Polen eine Versteigerung des 3,6-GHz-Bands an, das bis zum 30. Juni 2020 vergeben werden sollte. Nach dem Ausbruch der Pandemie beschlossen die polnischen Behörden, alle Verwaltungsverfahren für die Dauer der Pandemie auszusetzen. Im September 2021 war das Verfahren für die Versteigerung dieses Bands noch nicht abgeschlossen.

- In Spanien hätte die Versteigerung des 700-MHz-Bands ursprünglich im März 2020 stattfinden sollen. Den spanischen Behörden zufolge verzögerte sich aufgrund der COVID-19-Pandemie die Freigabe dieses Bands, das für das digitale Fernsehen genutzt wird. So wurde die Versteigerung zunächst auf Mai 2020 und dann auf das erste Quartal 2021 verschoben. Nach einer spanischen Gesetzesänderung im April 2021, bei der die Laufzeit der Lizenzen an den europäischen Kodex für die elektronische Kommunikation angeglichen wurden, kam es zu einer Verschiebung der Versteigerung auf den Sommer 2021, und die Vergabe des 700-MHz-Bands fand schließlich im Juli 2021 statt.

43 Ein weiterer Grund für Verzögerungen bei der Zuweisung der 5G-Pionierbänder sind die unterschiedlichen Ansätze der Mitgliedstaaten in Bezug auf die 5G-Sicherheit und die Verzögerungen bei der Verabschiedung ihrer Gesetze zur 5G-Sicherheit, die die Wirtschaft verunsichern (siehe Ziffern ***74*** und ***75***):

- In Spanien umfassten die Vorschriften für die Versteigerung von Pionierbändern eine allgemeine Klausel, wonach die Inhaber öffentlicher Konzessionen alle Verpflichtungen zur Sicherheit von 5G-Netzen einhalten müssen, die künftig zu irgendeinem Zeitpunkt in europäischen oder spanischen Verordnungen niedergelegt werden. Der vom Hof befragte spanische Mobilfunknetzbetreiber war der Ansicht, dass diese Klausel ihn verpflichtet, unter unsicheren Bedingungen Entscheidungen über Strategien und Käufe zu treffen. Außerdem wies er darauf hin, dass die nationalen Behörden nicht bereit seien, bestimmte wesentliche Bedingungen zu klären, wie etwa die Möglichkeit einer Entschädigung, wenn die künftigen Rechtsvorschriften, die bis Ende 2022 verabschiedet werden sollten, sie verpflichteten, ihre Ausrüstung zu ersetzen.

- In Polen war die Verschiebung der Zuweisung der 5G-Frequenzen u. a. darauf zurückzuführen, dass noch kein Gesetz zur Klärung der Sicherheitsanforderungen für 5G-Netze vorlag.

Weitere Anstrengungen sind erforderlich, um Sicherheitsprobleme bei der 5G-Einführung anzugehen

44 Im Hinblick auf Sicherheitsaspekte bei 5G untersuchte der Hof,

- ob die Kommission die erforderlichen Schritte unternommen hat, um eine solide Gestaltung des Sicherheitsrahmens zu fördern, und ob sie die Mitgliedstaaten angemessen unterstützt;

- ob die Mitgliedstaaten sichere 5G-Netze einrichten und sich dabei abstimmen, die im EU-Instrumentarium für die 5G-Cybersicherheit (Toolbox) enthaltenen Abhilfemaßnahmen verabschieden und ihre Rechtsvorschriften aktualisieren.

Die Kommission hat rasch reagiert, als ernsthafte Bedenken hinsichtlich der 5G-Sicherheit auf EU-Ebene aufkamen

45 Der 5G-Aktionsplan 2016 umfasst keine Sicherheitserwägungen. Die Sicherheit von 5G-Netzen und eine übermäßige Abhängigkeit von Anbietern aus Drittländern, insbesondere China, wurden im März 2019 als kritisches Problem ermittelt. In seiner Entschließung vom 12. März 2019[32] äußerte das Europäische Parlament die Sorge, dass 5G-Anbieter aus Nicht-EU-Ländern aufgrund der in diesen Ländern geltenden Gesetze ein Sicherheitsrisiko für die EU darstellen könnten. Am selben Tag wies die Kommission in ihren strategischen Perspektiven für die Beziehungen zwischen der EU und China darauf hin, dass ein gemeinsamer Ansatz der EU für die Sicherheit von 5G-Netzen notwendig sei, um sich vor möglichen schwerwiegenden Auswirkungen auf die Sicherheit kritischer digitaler Infrastrukturen zu schützen[33]. In seinen Schlussfolgerungen vom 21. und 22. März 2019 forderte der Europäische Rat die Kommission auf, eine Empfehlung zu einem abgestimmten Vorgehen bei der Sicherheit von 5G-Netzen abzugeben[34].

46 Einige Tage später gab die Kommission eine solche Empfehlung mit einer Reihe von Maßnahmen sowohl auf nationaler Ebene (z. B. Risikobewertung zu 5G) als auch auf EU-Ebene (z. B. koordinierte Risikobewertung) ab, mit denen ein hohes Maß an Cybersicherheit von 5G-Netzen in der gesamten EU sichergestellt werden soll[35].

47 Fast alle Mitgliedstaaten hatten ihre nationalen Risikobewertungen bis zum Juli 2019 abgeschlossen[36]. Im Oktober 2019 veröffentlichte die NIS-Kooperationsgruppe einen Bericht über die EU-weit koordinierte Risikobewertung zur Cybersicherheit in

---

[32] Entschließung des Europäischen Parlaments vom 12. März 2019 (2019/2575(RSP)).

[33] JOIN(2019) 5 final vom 12.3.2019. EU-China – A strategic outlook.

[34] Schlussfolgerungen des Europäischen Rates vom 21. und 22. März 2019.

[35] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 "Cybersicherheit der 5G-Netze".

[36] Pressemitteilung vom 19. Juli 2019.

5G-Netzen, und das "EU-Instrumentarium für die 5G-Cybersicherheit"[37] wurde im Januar 2020 veröffentlicht (siehe ***Anhang VII***). Kurz darauf wurde es von der Kommission und dem Europäischen Rat gebilligt[38].

Mit dem EU-Instrumentarium für die 5G-Cybersicherheit aus dem Jahr 2020 wurden erstmals Maßnahmen zur Bewältigung von Sicherheitsbedrohungen auf EU-Ebene ohne präskriptiven Charakter eingeführt

Dass die Sicherheit von 5G-Netzen als nationale Sicherheitskompetenz behandelt wird, schränkt den Handlungsspielraum der Kommission ein

48 In den EU-Verträgen[39] sind die Handlungsmöglichkeiten festgelegt, um Herausforderungen wie den Aufbau sicherer 5G-Netze auf EU-Ebene zu bewältigen. Dieser Umfang ist weit gefasst und lässt der Kommission und den Mitgliedstaaten einen gewissen Auslegungsspielraum (siehe ***Kasten 4***).

[37] Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures. NIS Cooperation Group, 01/2020.

[38] Mitteilung der Europäischen Kommission, Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums, COM(2020) 50 final; Schlussfolgerungen des Europäischen Rates vom 1. und 2. Oktober 2020 (EUCO 13/20).

[39] Vertrag über die Arbeitsweise der Europäischen Union.

Kasten 4

Zuständigkeiten der EU in Bezug auf 5G-Netze: geteilte Zuständigkeit oder eine Frage der nationalen Sicherheit?

Die Zuständigkeit für den EU-Binnenmarkt erstreckt sich grundsätzlich auch auf 5G-Netze (als geteilte Zuständigkeit), und zwar als Dienst (Bereitstellung eines Dienstes durch Mobilfunknetzbetreiber) und als Ware (die 5G-Ausrüstung selbst, die von den Mobilfunknetzbetreibern für den Aufbau ihrer 5G-Netze erworben wurde). Im Rahmen der geteilten Zuständigkeit kann die EU (die Kommission und andere Organe der Union) rechtsverbindliche Maßnahmen (Rechtsvorschriften) erlassen, um die Verwirklichung des Binnenmarktes zu gewährleisten und sein reibungsloses Funktionieren zu fördern. Die Sicherheit der 5G-Netze könnte im weiteren Sinne auch als Teil des Raums der Freiheit, der Sicherheit und des Rechts der EU betrachtet werden. In diesem Sinne kann Sicherheit als ein allgemeiner Begriff im Zusammenhang mit der Verhütung und Bekämpfung von Kriminalität verstanden und damit als eine weitere geteilte Zuständigkeit gesehen werden, für die die EU rechtsverbindliche Maßnahmen verabschieden kann.

Andererseits würde eine engere Auslegung des Begriffs der Sicherheit darin bestehen, ihn auf Bedrohungen der nationalen Sicherheit der Mitgliedstaaten zu beschränken. In diesem Fall wäre eine ausschließlich nationale Zuständigkeit gegeben, bei der die EU nur ergänzend tätig werden könnte, um die nationalen Bemühungen der Mitgliedstaaten zur Gewährleistung der Sicherheit ihrer 5G-Netze zu unterstützen.

49 Die Sicherheit von 5G-Netzen erstreckt sich über nationale und EU-Kompetenzen und betrifft die nationale Sicherheit. Die Kommission hat die Sicherheit von 5G-Netzen als Bedrohung für die nationale Sicherheit behandelt und sich daher für die Option "nicht zwingender" Maßnahmen entschieden. Dies bedeutet, dass der EU die Möglichkeit fehlt, rechtlich bindende Maßnahmen zu erlassen, die die Mitgliedstaaten zur Anwendung einheitlicher Risikominderungsmaßnahmen oder zur Einführung durchsetzbarer Anforderungen verpflichten würden. Die Kommission kann stattdessen unverbindliche Empfehlungen und Mitteilungen veröffentlichen, zur Verbreitung bewährter Verfahren beitragen und die nationalen Maßnahmen der Mitgliedstaaten koordinieren. Allerdings kommt noch ein weiterer Ansatz in Betracht. Ein solches Beispiel ist die NIS-Richtlinie[40], bei der es sich um einen EU-Rechtsakt handelt, der sich

[40] Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

auf die Sicherheit von Netz- und Informationssystemen in der gesamten Union bezieht. Dieser Rechtsakt wurde von der Kommission vorgeschlagen und auf der binnenmarktbezogenen Rechtsgrundlage verabschiedet, obwohl die Cybersicherheit weitgehend ein nationales Vorrecht ist[41].

Das EU-Instrumentarium für die 5G-Cybersicherheit wurde zwar in einer frühen Einführungsphase angenommen, einige Mobilfunknetzbetreiber hatten ihre Anbieter jedoch bereits ausgewählt

50 Im Januar 2020 nahm die NIS-Kooperationsgruppe ein EU-Instrumentarium für die 5G-Cybersicherheit an, in dem verschiedene strategische, technische und Unterstützungsmaßnahmen zur Bewältigung von Bedrohungen für die Sicherheit von 5G-Netzen aufgeführt und für jede dieser Maßnahmen die zuständigen Akteure benannt werden. Die Annahme dieses von der Kommission und dem Europäischen Rat gebilligten Instrumentariums erfolgte nur neun Monate, nachdem das Europäische Parlament und der Rat erstmals ihre Bedenken hinsichtlich der 5G-Sicherheit geäußert hatten. In jüngerer Zeit wurde das EU-Instrumentarium für die 5G-Cybersicherheit in der neuen europäischen Strategie zur Förderung intelligenter, sauberer und sicherer Verbindungen in digitalen Systemen in der ganzen Welt als Instrument zur Lenkung von Investitionen in digitale Infrastruktur erwähnt[42]. Der von der Kommission verfolgte Soft-Law-Ansatz hat dazu beigetragen, dass auch auf EU-Ebene rasch Maßnahmen zur Bewältigung von Sicherheitsbedrohungen in die Wege geleitet wurden und die Zusammenarbeit der Mitgliedstaaten in diesem grenzüberschreitenden Bereich erleichtert wurde. Zum Vergleich: Bei der NIS-Richtlinie dauerte es von der Vorlage des Kommissionsvorschlags[43] bis zu seiner Annahme[44] mehr als drei, bei der EECC-Richtlinie mehr als zwei Jahre[45]. Die Umsetzung der Richtlinien in den nationalen Rechtssystemen der Mitgliedstaaten nahm sogar noch mehr Zeit in Anspruch (siehe auch Ziffern ***36*** und ***37***).

---

[41] Analyse Nr. 02/2019 "Herausforderungen für eine wirksame Cybersicherheitspolitik der EU (Themenpapier)", Ziffer 36.

[42] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – The Global Gateway. JOIN(2021) 30 final vom 1.12.2021.

[43] COM(2013) 48 final vom 7.2.2013.

[44] Richtlinie (EU) 2016/1148.

[45] COM(2016) 590 final/2 vom 12.10.2016 und Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

51 Das EU-Instrumentarium für die 5G-Cybersicherheit wurde vier Jahre nach der Vorstellung der 5G-Strategie im Rahmen des 5G-Aktionsplans angenommen, und im selben Jahr hätten im Rahmen dieses Aktionsplans Etappenziele für die 5G-Einführung erreicht werden sollen. In diesem Zusammenhang vertraten die für diese Prüfung befragten Vertreter der Ministerien der Mitgliedstaaten, der nationalen Regulierungsbehörden und der Mobilfunknetzbetreiber die Ansicht, dass mit der Durchführung der Maßnahmen im Bereich der 5G-Sicherheit zu spät begonnen worden sei.

52 Gleichzeitig wurde das Instrumentarium veröffentlicht, als sich die 5G-Einführung und die Pläne in den meisten Mitgliedstaaten noch in einem frühen Stadium befanden. Die meisten Verträge zwischen Anbietern und Betreibern von 5G-Ausrüstung wurden 2020 und 2021 abgeschlossen. Nach Angaben des Europäischen Verbands der Telekommunikationsbetreiber (ETNO) hatten jedoch einige Mobilfunknetzbetreiber bereits Anbieter ausgewählt, als das EU-Instrumentarium für die 5G-Cybersicherheit bereitgestellt wurde.

Das EU-Instrumentarium für die 5G-Cybersicherheit stellte zwar einen Rahmen für die Bewertung des Risikoprofils der Anbieter zur Verfügung, es gibt jedoch weiterhin Schwachstellen

Einige Mitgliedstaaten und nationale Behörden sind der Ansicht, dass einige der Kriterien für die Einstufung von Anbietern als Hochrisikoanbieter nicht eindeutig genug sind

53 Ein zentrales Element des EU-Instrumentariums für die 5G-Cybersicherheit ist das Erfordernis, dass die Mitgliedstaaten die Anbieter bewerten und bei als kritisch eingestuften wichtigen Anlagen und Einrichtungen Beschränkungen auf Anbieter anwenden, die als Hochrisikoanbieter eingestuft sind. Die Mitgliedstaaten sollten diese Bewertung auf der Grundlage einer nicht erschöpfenden Liste von Kriterien durchführen, die sich aus der von der EU koordinierten Risikobewertung ergeben. Zu diesen Kriterien zählen beispielsweise:

- die Wahrscheinlichkeit, dass ein Anbieter Eingriffen vonseiten eines Nicht-EU-Staates unterliegt, z. B. durch das Bestehen einer engen Verbindung zwischen dem Anbieter und der Regierung eines Nicht-EU-Staates oder durch dessen Gesetzgebung, insbesondere wenn es keine gesetzgeberischen und demokratisch legitimierten Kontroll- und Einflussrechte gibt oder in Ermangelung von Sicherheits- oder Datenschutzabkommen zwischen der EU und dem betreffenden Staat;

- die Gewährleistung der Versorgungssicherheit durch den Anbieter;
- die Gesamtqualität der Produkte und Cybersicherheitsverfahren des Anbieters.

54 Das Instrumentarium wurde entwickelt, um eine Fragmentierung zu vermeiden und die Kohärenz im Binnenmarkt zu fördern. Die in dem Instrumentarium festgelegten Kriterien bieten einen operativen Rahmen, der für die koordinierte Bewertung des Risikoprofils der Anbieter in allen Mitgliedstaaten hilfreich ist. Außerdem konnte die Kommission gemeinsam mit den Mitgliedstaaten rasch auf neue Bedenken hinsichtlich der 5G-Sicherheit reagieren. Gleichzeitig fällt es nach wie vor in die Zuständigkeit der nationalen Behörden, diese Kriterien bei der Bewertung der mit bestimmten Anbietern verbundenen Risiken anzuwenden. Bis Oktober 2021 hatten 13 Mitgliedstaaten unter Berücksichtigung dieses Rahmens ihre Rechtsvorschriften zur 5G-Sicherheit in Kraft gesetzt oder geändert (siehe Ziffer ***75*** und ***Abbildung 6***).

55 Die vom Hof befragten Vertreter von zwei der vier mitgliedstaatlichen Ministerien waren jedoch der Ansicht, dass einige der Kriterien für die Einstufung von 5G-Anbietern unterschiedlich ausgelegt werden können und einer weiteren Klärung bedürfen. Sie forderten die Kommission ferner auf, zusätzliche Unterstützung und Orientierungshilfen für die Einstufung von Hochrisikoanbietern bereitzustellen. Außerdem wiesen die befragten Vertreter der Mitgliedstaaten darauf hin, dass die Situation die Gefahr eines uneinheitlichen Vorgehens der Mitgliedstaaten in Bezug auf Hochrisikoanbieter birgt (siehe auch Ziffern ***74*** und ***75*** sowie ***Kasten 5***) Elf der nationalen Regulierungsbehörden, die an der Umfrage des Hofes teilnahmen und deren Engagement für die 5G-Sicherheit auf unterschiedlichem Niveau lag, äußerten ähnliche Bedenken.

Das Herkunftsland der 5G-Anbieter beeinflusst die Bewertung der Sicherheitsrisiken

56 Die 5G-Anbieter unterscheiden sich in ihren Geschäftsprofilen und kommen aus Ländern mit unterschiedlichen Verbindungen zur EU. ***Abbildung 5*** zeigt eine Reihe von Gemeinsamkeiten und Unterschieden zwischen den wichtigsten 5G-Anbietern und ihren Herkunftsländern, insbesondere in Bereichen, die dem Instrumentarium zufolge die Bewertung des Risikoprofils beeinflussen dürften (siehe Ziffer ***53***).

Abbildung 5 – 5G-Anbieter und ihre Herkunftsländer – Gemeinsamkeiten und Unterschiede

Quelle: Europäischer Rechnungshof, auf der Grundlage folgender Datensätze: WTO members; OECD members; OECD FDI Restrictiveness Index; Weltbank, Datensatz "Worldwide Governance Indicators, 2019; Weltwirtschaftsforum, Datensatz "Global Competitiveness", Ranking von 2018; Angemessenheitsbeschlüsse; Statista, Who is leading the 5G patent race?; Unternehmensdaten Ericsson; Unternehmensdaten Nokia; Unternehmensdaten Qualcomm; Unternehmensdaten Sharp; Unternehmensdaten LG; Unternehmensdaten Samsung; Unternehmensdaten Huawei; und Unternehmensdaten ZTE. Wechselkurse vom 31.12.2020.

57 Ein Risikofaktor ist, inwieweit das Herkunftsland eines Anbieters die zentralen politischen und wirtschaftlichen Werte der EU erfüllt. Länderspezifische Faktoren wie Rechtsstaatlichkeit, Unabhängigkeit der Justiz, Offenheit für ausländische Investitionen und das Bestehen von Datenschutzabkommen können als Maß für den rechtlichen Schutz eines Unternehmens vor staatlichen Eingriffen und den Schutz, den das Unternehmen seinen Kunden bieten kann, herangezogen werden.

58 Zwar sind in EU-Mitgliedstaaten ansässige Anbieter zur Einhaltung der Standards und rechtlichen Anforderungen der EU verpflichtet, dies gilt jedoch nicht für sechs der größten Anbieter, die ihren Sitz in Nicht-EU-Ländern haben und im Rahmen der in diesen Drittländern geltenden Rechtsvorschriften tätig sind (siehe ***Abbildung 5***). Diese Rechtsvorschriften können sich erheblich von den EU-Standards unterscheiden, z. B. im Hinblick auf den Datenschutz für die Bürgerinnen und Bürger und die Wirksamkeit dieses Schutzes oder ganz allgemein darauf, wie die Unabhängigkeit der Justiz durch gesetzgeberische und demokratisch legitimierte Kontroll- und Einflussrechte gewährleistet wird. Was die Unabhängigkeit der Justiz anbelangt, so schneiden die USA und Japan besser ab als andere Nicht-EU-Herkunftsländer von 5G-Anbietern, während Südkorea unter den Nicht-EU-Ländern in Bezug auf die Rechtsstaatlichkeit die besten Ergebnisse vorweisen kann.

59 5G-Netze werden vornehmlich über Software betrieben. Die Tatsache, dass einige Anbieter im Rahmen der Gesetzgebung von Nicht-EU-Ländern tätig sind, gibt insbesondere dann Anlass zu Bedenken, wenn die Kontrollzentren für die Software ebenfalls außerhalb der EU angesiedelt sind, was dazu führen kann, dass EU-Nutzer der Gesetzgebung von Nicht-EU-Ländern unterliegen.

60 Die Kommission hat damit begonnen, sich dieser Probleme anzunehmen, und vertritt die Ansicht, dass alle Unternehmen, die Dienstleistungen für EU-Bürger erbringen, die Regeln und Werte der EU einhalten sollten[46]. Sie ist mit mehreren Ländern in einen Dialog getreten, um einen starken Schutz personenbezogener Daten zu gewährleisten[47]. ***Abbildung 5*** zeigt auch, dass die Kommission die Angemessenheit des japanischen (und in der Vergangenheit des US-amerikanischen) Datenschutzsystems bereits anerkannt hat. Es sei jedoch darauf hingewiesen, dass Angemessenheitsbeschlüsse anfechtbar sind und einer strengen gerichtlichen

---

[46] Mitteilung der Europäischen Kommission, Gestaltung der digitalen Zukunft Europas, COM(2020) 67 final.

[47] EU-China – A strategic outlook.

Kontrolle unterliegen. So lehnte der Gerichtshof der Europäischen Union im Jahr 2015 das damals anwendbare Rechtsinstrument für den Datenaustausch mit den Vereinigten Staaten, die "Safe-Harbor-Regelung"[48], ab und entschied später im Jahr 2020, dass der Datenschutzschild (der das Safe-Harbor-Abkommen ersetzt hatte) EU-Bürgern keinen angemessenen Schutz bietet[49]. Für die Vereinigten Staaten liegt daher derzeit kein Angemessenheitsbeschluss vor. Ganz allgemein und über das Bestehen einer Datenschutzregelung hinaus ist es wichtig, den breiteren rechtlichen und institutionellen Rahmen zu berücksichtigen, einschließlich beispielsweise der Achtung der Rechtsstaatlichkeit und der Art und Weise, wie die Unabhängigkeit der Justiz gewährleistet wird.

61 Aus ***Abbildung 5*** geht außerdem hervor, dass es zwischen den 5G-Anbietern in Bezug auf den Anteil der 5G-Patente, die Einnahmen und die Beschäftigtenzahl große Unterschiede gibt. Dies wirkt sich auf die Ressourcen aus, die ihnen zur Verfügung stehen, was wiederum ihre Widerstandsfähigkeit und ihre Fähigkeit, eine kontinuierliche Versorgung sicherzustellen, beeinträchtigen kann. Beispielsweise sind Samsung und Huawei die Anbieter, die den höchsten Anteil an 5G-Patenten haben, die höchsten Unternehmensumsätze erzielen und insgesamt die meisten Mitarbeiter beschäftigen.

62 Die Wahrscheinlichkeit, dass ein Anbieter Eingriffen vonseiten der Regierung eines Nicht-EU-Staates unterliegt, ist ein weiterer wichtiger Faktor, der gemäß dem Instrumentarium das Risikoprofil eines Anbieters bestimmt. In diesem Zusammenhang spielen die Eigentumsverhältnisse eine wichtige Rolle, da Anteilseigner mit umfangreicher Beteiligung möglicherweise Druck ausüben oder Entscheidungen des Managements beeinflussen können. Außerdem wird davon ausgegangen, dass in privatem oder staatlichem Eigentum stehende Unternehmen einer öffentlichen Kontrolle im Wege von Prüfungen und Rechenschaftspflicht weniger offen gegenüberstehen als börsennotierte Unternehmen mit breit gestreuter Beteiligung, bei denen zum Vorteil der Anleger und der Regulierungsbehörden ganzjährig strenge Offenlegungspflichten bestehen. Die meisten 5G-Anbieter sind entweder in ihrem Herkunftsland oder im Ausland an einer Börse notiert, während die chinesischen

---

[48] Urteil in der Rechtssache C-362/14 und https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[49] Urteil in der Rechtssache C-311/18 und https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

Anbieter schwieriger zu klassifizieren sind und allgemein von einer engen Verbindung dieser Unternehmen zur chinesischen Regierung ausgegangen wird[50].

Nach Ansicht der Mitgliedstaaten war die Unterstützung der Kommission und der ENISA bei der Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit von Nutzen

63 Die Kommission unterstützte die Mitgliedstaaten durch den Austausch bewährter Verfahren zu einigen Schlüsselmaßnahmen des EU-Instrumentariums für die 5G-Cybersicherheit, etwa in Bezug auf Hochrisikoanbieter. Diese Unterstützung, die häufig im Rahmen der NIS-Kooperationsgruppe erfolgte, wurde durch spezifische Maßnahmen der ENISA ergänzt, die beispielsweise Webinare organisierte oder zu folgenden Aspekten Orientierungshilfen bereitstellte:

- Umsetzung des Instrumentariums mit einem Schwerpunkt auf den technischen Maßnahmen;
- bewährte Verfahren im Bereich der Netzsicherheit, insbesondere für
  - 5G-Bedrohungslagen[51];
  - die Ausarbeitung nationaler Risikobewertungen zu 5G;
  - Sicherheitsmaßnahmen im Rahmen des Europäischen Kodex für die elektronische Kommunikation[52], einschließlich spezieller Leitlinien zur 5G-Sicherheit[53].

64 Die Kommission beauftragte die ENISA ferner mit der Ausarbeitung des EU-Schemas für die Cybersicherheitszertifizierung von 5G-Netzen, das dazu beitragen sollte, Risiken im Zusammenhang mit ihren technologischen Schwachstellen anzugehen und die Cybersicherheit weiter zu verbessern[54]. Diese Zertifizierung könnte zwar zur Verbesserung der Sicherheit beitragen, sie kann jedoch nicht verhindern, dass Bedrohungen durch Software-Updates in die Systeme integriert werden.

---

[50] https://www.europarl.europa.eu/doceo/document/E-9-2020-004305_DE.html und https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

[51] ENISA, Threat Landscape for 5G Networks, 14.12.2020.

[52] ENISA, Guideline on Security Measures under the EECC, 10.12.2020.

[53] ENISA, 5G supplement to the Guidelines on Security Measures under the EECC, 07.07.2021.

[54] Pressemitteilung vom 3. Februar 2021.

65 Alle Vertreter der Behörden der Mitgliedstaaten, die der Hof im Rahmen seiner Prüfung befragt hat, betonten den Nutzen der Unterstützung der Kommission und der ENISA bei der Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit. Darüber hinaus gaben die meisten nationalen Regulierungsbehörden für Telekommunikation (15 von 21) an, dass die Kommission und/oder die ENISA die nationalen Behörden beim Austausch bewährter Verfahren für die Umsetzung strategischer Schlüsselmaßnahmen unterstützt hätten.

Die Annahme des EU-Instrumentariums für die 5G-Cybersicherheit erfolgte zu spät, sodass es bei von der EU kofinanzierten Projekten im Zeitraum 2014-2020 nicht berücksichtigt wurde

66 Eines der Ziele des EU-Instrumentariums für die 5G-Cybersicherheit besteht darin, sicherzustellen, dass die von der EU kofinanzierten 5G-Projekte den Cybersicherheitsrisiken Rechnung tragen. Das Instrumentarium wurde allerdings erst im Januar 2020 angenommen. Da alle vom Hof im Rahmen dieser Prüfung überprüften Projekte ausgewählt worden waren, bevor das EU-Instrumentarium für die 5G-Cybersicherheit angenommen wurde, konnte nicht davon ausgegangen werden, dass bei ihnen der empfohlene Ansatz für Cybersicherheit, auch gegenüber Hochrisikoanbietern, befolgt wurde. So ermittelte der Hof beispielsweise in seiner Stichprobe ein Projekt des Programms Horizont 2020 und zwei EFRE-Projekte in Spanien, bei denen chinesische 5G-Ausrüstung zum Einsatz kam, die anschließend in Schweden verboten wurde (siehe Ziffer ***15***).

67 Für den Zeitraum 2021-2027 beabsichtigt die Kommission, einen kohärenten Ansatz für die 5G-Sicherheit für von der EU kofinanzierte Projekte zu fördern, indem sie sicherstellt, dass die Einhaltung des Instrumentariums eine Voraussetzung für die EU-Finanzierung ist. Dies wird jedoch von der Art der Umsetzung abhängen:

- Bei unmittelbar von der Kommission verwalteten Programmen (z. B. Horizont Europa 2021-2027) können Anbieter ausgeschlossen werden, die Eingriffen seitens der Regierung eines Nicht-EU-Landes unterliegen. Dies dürfte dazu führen, dass EU-finanzierte Projekte den Cybersicherheitsrisiken Rechnung tragen und Situationen verhindert werden, in denen ein Anbieter, der in einem Mitgliedstaat eine Kofinanzierung erhält, in einem anderen Mitgliedstaat als Hochrisikoanbieter eingestuft und ausgeschlossen wird.

- Bei Programmen, die im Rahmen der geteilten Mittelverwaltung durchgeführt werden, enthalten die Rechtsvorschriften keine Anforderungen in Bezug auf Cybersicherheitsrisiken, weshalb die Kommission verstärkt auf die Aufnahme einer Bezugnahme auf das Instrumentarium in Partnerschaftsvereinbarungen

achten will, um sicherzustellen, dass Cybersicherheitsrisiken bei der Finanzierung von 5G-Projekten aus dem EFRE berücksichtigt werden.

- Für InvestEU (das Programm, das den EFSI ersetzt)[55] und die Aufbau- und Resilienzfazilität plant die Kommission, die zuständigen Stellen dazu anzuhalten, in Finanzierungsvereinbarungen auf das EU-Instrumentarium Bezug zu nehmen.

Bei der Einführung von 5G-Netzen gibt es noch kein abgestimmtes Vorgehen der Mitgliedstaaten in Bezug auf Sicherheitsaspekte

Die Informationen über die Behandlung von Sicherheitsfragen durch die Mitgliedstaaten sind unzureichend

68 Die Kommission verfolgt die Fortschritte bei der Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit über die NIS-Kooperationsgruppe, über bilaterale Gespräche mit den Mitgliedstaaten und indirekt über die Medien und erstattet darüber Bericht. Die ersten Ergebnisse dieser Überwachung wurden im Juli 2020 veröffentlicht[56]. Im Dezember 2020 veröffentlichte die Kommission ferner einen Bericht über die Auswirkungen ihrer Empfehlung zur Cybersicherheit von 5G-Netzen[57]. Bis September 2021 gab es keine Pläne für weitere Berichte.

69 Die oben genannten Berichte enthalten jedoch keine gemeinsamen zentralen Leistungsindikatoren und keine vergleichbaren detaillierten Informationen über das Vorgehen der Mitgliedstaaten im Hinblick auf 5G-Sicherheitsbedenken.

70 Außerdem gibt es kaum öffentlich verfügbare Informationen darüber, welchen Ansatz die Mitgliedstaaten in Bezug auf Hochrisikoanbieter verfolgen (d. h. wie diese ermittelt werden), und über den möglichen Ausschluss von Anbietern bei der Bereitstellung von 5G-Ausrüstung. Wenn überhaupt Informationen vorliegen, sind diese widersprüchlich und unvollständig. Zur Illustration:

- In ihrem Bericht von Juli 2020 über die Fortschritte der Mitgliedstaaten bei der Umsetzung des EU-Instrumentariums (siehe Ziffer ***68***) stellt die Kommission fest,

---

[55] Verordnung (EU) 2021/523 zur Einrichtung des Programms "InvestEU".

[56] Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, Juli 2020.

[57] Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final vom 16.12.2020.

dass etwa die Hälfte der Mitgliedstaaten (14 von 27) das Risikoprofil der Anbieter bewertet und denjenigen Beschränkungen auferlegt hatte, die als Anbieter mit hohem Risikoprofil eingestuft wurden.

- In einem Bericht von Dezember 2020[58] wies das GEREK darauf hin, dass nur neun Mitgliedstaaten solche Beschränkungen eingeführt hätten und dass sieben der übrigen 18 Mitgliedstaaten nicht beabsichtigten, sie in Zukunft einzuführen.

71 Selbst wenn die Mitgliedstaaten Rechtsvorschriften zur Sicherheit von 5G-Netzen erlassen haben (siehe auch Ziffer ***75***), geben diese keinen Aufschluss über den Ansatz der Mitgliedstaaten gegenüber Hochrisikoanbietern. Konkrete Entscheidungen dürften wohl nur im Wege von Durchführungsrechtsakten oder nicht öffentlichen Verwaltungs- oder Geschäftsentscheidungen getroffen werden.

72 Den vom Hof befragten Interessenträgern und Entscheidungsträgern (z. B. im Europäischen Parlament) zufolge mangelt es ebenfalls an nicht öffentlichen Informationen (z. B. durch Berichte der Kommission oder der NIS-Gruppe) über den Ansatz der Mitgliedstaaten gegenüber Hochrisikoanbietern, weshalb diese Akteure sich auf Medien und inoffizielle Quellen stützen müssen.

73 Obwohl die Bedenken hinsichtlich der 5G-Sicherheit von Natur aus grenzübergreifend sind, liegen der Öffentlichkeit insgesamt kaum Informationen darüber vor, wie die Mitgliedstaaten Sicherheitsfragen angehen, insbesondere was Hochrisikoanbieter betrifft. Dies behindert den Wissensaustausch zwischen den Mitgliedstaaten und die Möglichkeit, abgestimmte Maßnahmen durchzuführen. Zudem schränkt es die Möglichkeiten der Kommission ein, Verbesserungen der Sicherheit von 5G-Netzen vorzuschlagen.

Es gibt Hinweise darauf, dass einige Mitgliedstaaten unterschiedliche Ansätze gegenüber 5G-Anbietern verfolgen

74 Die nationalen Behörden verfügen bei der Durchführung von Schlüsselmaßnahmen im Bereich der 5G-Sicherheit über einen großen Ermessensspielraum (siehe Ziffern ***48*** und ***49***). Das Instrumentarium berücksichtigt nationale Zuständigkeiten und relevante länderspezifische Faktoren (Bedrohungsbewertung durch nationale Sicherheitsdienste, Zeitrahmen für die Einführung von 5G, Präsenz von Anbietern, Cybersicherheitskapazitäten). Bislang

[58] GEREK, "Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)", BoR 20 (227), 10.12.2020.

haben die Mitgliedstaaten in Bezug auf die Nutzung von Ausrüstung bestimmter Anbieter oder den Umfang der Beschränkungen für Hochrisikoanbieter unterschiedliche Ansätze verfolgt (siehe Beispiele von vier Mitgliedstaaten in ***Kasten 5***).

Kasten 5

Beispiele für unterschiedliche Ansätze der Mitgliedstaaten gegenüber chinesischen 5G-Anbietern

Rahmen vorhanden und Beschränkungen werden angewandt[(1)]

Im Oktober 2020 legte die schwedische Regulierungsbehörde für den Telekommunikationssektor (PTS) folgende Bedingungen für die Teilnahme an der Versteigerung von 5G-Frequenzen fest:

— Bei neuen Installationen und der Implementierung zentraler Funktionen für die Funknutzung in den Frequenzbändern dürfen keine Produkte chinesischer Anbieter verwendet werden.

— Alle bestehenden Infrastrukturen dieser Anbieter müssen spätestens zum 1. Januar 2025 außer Betrieb gesetzt werden.

Rahmen vorhanden, aber noch nicht angewandt[(2), (3), (4)]

In Deutschland sieht das IT-Sicherheitsgesetz 2.0 von Mai 2021 eine obligatorische Zertifizierung kritischer Komponenten vor, bevor ihr Einsatz genehmigt werden kann. Die vom Hof befragten deutschen Mobilfunknetzbetreiber würden ein einheitliches europäisches Zertifizierungsverfahren mit einheitlicher europäischer Anlaufstelle unter Federführung der ENISA vorziehen, anstatt eine potenzielle Vielzahl nationaler Zertifizierungen durchlaufen zu müssen. Das Gesetz erlaubt es dem Bundesministerium des Innern auch, den Einsatz kritischer Komponenten zu verbieten, wenn diese eine Gefahr für die nationale Sicherheit darstellen könnten.

Das aktualisierte Telekommunikationsgesetz ermöglicht es dem zuständigen Minister, Anbieter als "Hochrisikoanbieter" einzustufen und Beschränkungen auf sie anzuwenden oder sie vom Markt auszuschließen. Aus öffentlich zugänglichen Informationen von Oktober 2021 geht hervor, dass das Land dabei ist, sein 5G-Netz mithilfe des chinesischen Anbieters Huawei auszubauen.

Kein Rahmen vorhanden[5], [6]

Mit Stand von September 2021 hat Ungarn keine Beschränkungen für 5G-Anbieter angewandt und wird dies wahrscheinlich auch in naher Zukunft nicht tun. Ungarn hat auch offiziell die Teilnahme an dem von den USA geförderten internationalen *5G Clean Network Program* abgelehnt, das darauf abzielt, die Präsenz chinesischer Anbieter in 5G-Kernnetzen zu begrenzen.

(1) Decision 18-8496 of 20.10.2020 on the terms for the auction for frequency bands 3.5 GHz and 2.3 GHz.

(2) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

(3) Österreichisches Telekommunikationsgesetz.

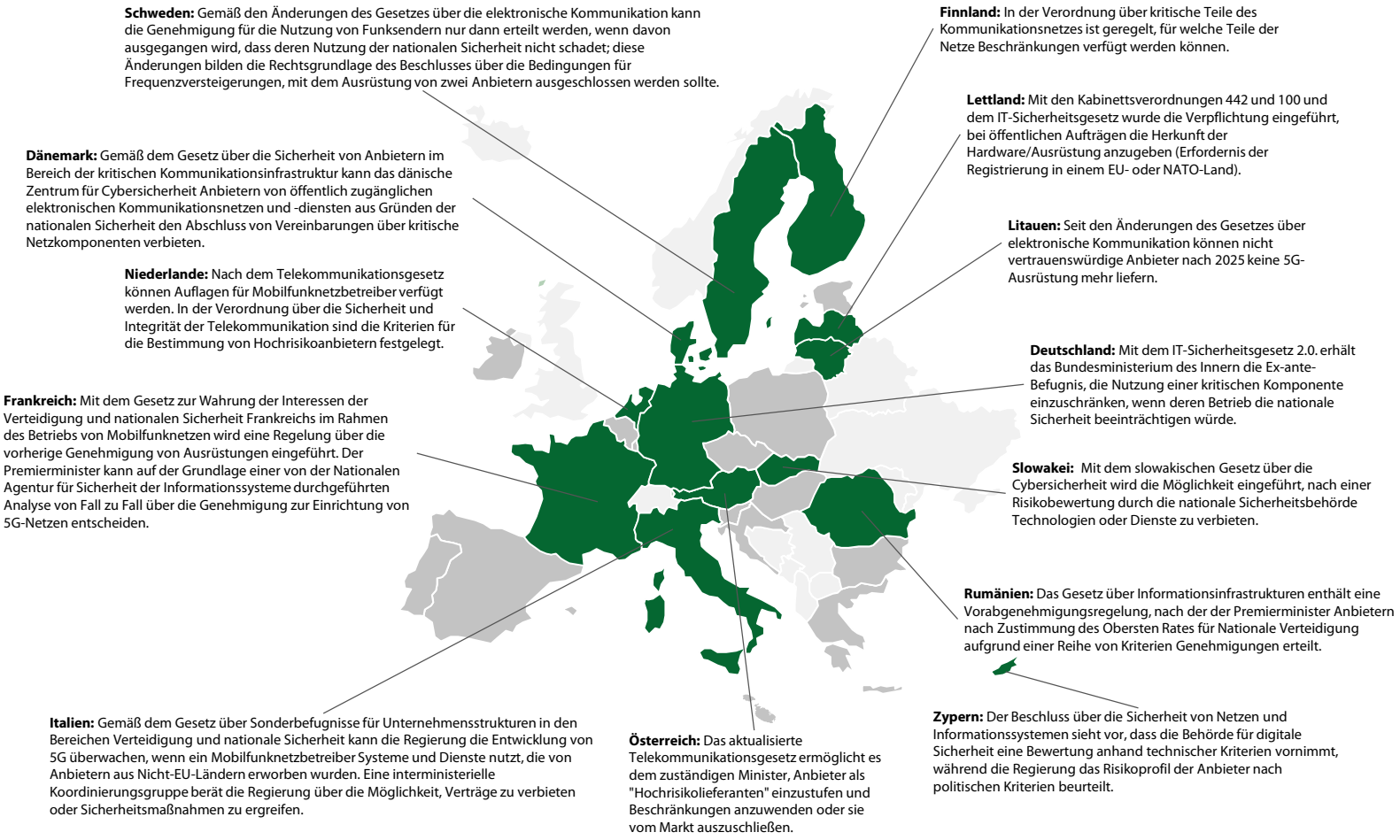
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(5) https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf

(6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/hungary

75 Seit der Annahme des Instrumentariums wurden bei der Erhöhung der Sicherheit von 5G-Netzen Fortschritte erzielt, wobei die meisten Mitgliedstaaten Hochrisikoanbietern Beschränkungen auferlegt haben oder dabei sind, dies zu tun. Bis Ende 2021 hatten 13 Mitgliedstaaten nationale Gesetze zur 5G-Sicherheit verabschiedet oder geändert. Diese Regulierungsmaßnahmen tragen den im Instrumentarium festgelegten Kriterien Rechnung, folgen jedoch unterschiedlichen Ansätzen (siehe ***Abbildung 6***). Andere Mitgliedstaaten sind dabei, entsprechende Rechtsvorschriften vorzulegen. In den kommenden Jahren könnte dies zu einheitlicheren Ansätzen gegenüber 5G-Hochrisikoanbietern führen, zumindest unter den Mitgliedstaaten, die entsprechende Rechtsvorschriften erlassen haben.

Abbildung 6 – Mitgliedstaaten, die Rechtsvorschriften erlassen haben, die es ermöglichen, Ausrüstung von Hochrisikoanbietern aus ihren Netzen auszuschließen, Oktober 2021



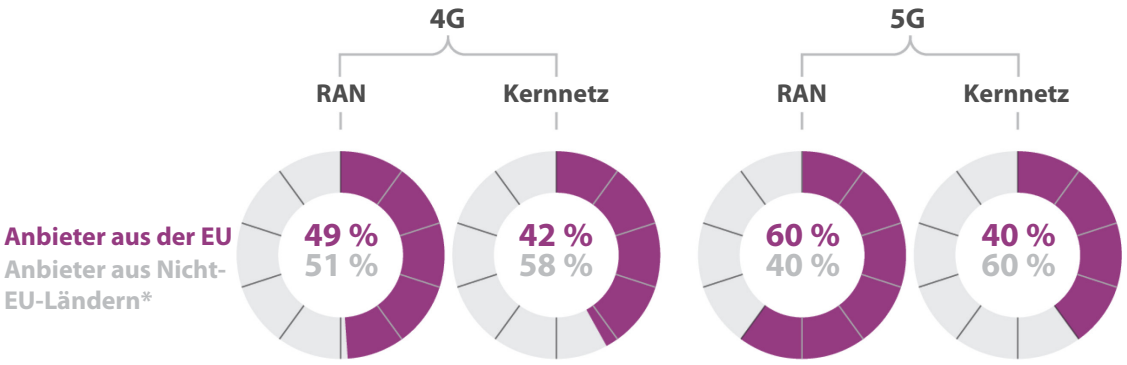
Quelle: Europäischer Rechnungshof auf der Grundlage von Daten der Europäischen Kommission.

76 Bislang hat die Kommission nicht bewertet, welche Auswirkungen solche voneinander abweichenden Ansätze haben würden, wenn ein Mitgliedstaat seine 5G-Netze unter Verwendung von Ausrüstung eines Anbieters aufbaut, der in einem anderen Mitgliedstaat als Hochrisikoanbieter eingestuft ist. Dies könnte sich entweder auf die grenzüberschreitende Sicherheit oder den Wettbewerb zwischen im EU-Binnenmarkt tätigen Mobilfunknetzbetreibern auswirken.

Die Kommission hat vor Kurzem begonnen, sich mit der Frage ausländischer Subventionen zu befassen, die den Binnenmarkt verzerren

77 Mit Stand von Dezember 2020 wurde mehr als die Hälfte aller 4G- und 5G-Ausrüstungen in der EU von Nicht-EU-Anbietern bezogen (siehe ***Abbildung 7***).

Abbildung 7 – Anteil der Mobilfunknetzbetreiber, die Ausrüstung von Anbietern aus EU-/Nicht-EU*-Ländern verwenden



* *Die Nicht-EU-Länder umfassen Nordamerika, Asien und Australien.*

Quelle: Europäischer Rechnungshof auf der Grundlage des GEREK. "Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)". BoR (20) 227.

78 Insbesondere nutzten Ende 2019 286 Millionen Kunden in der EU-27 (64 % der Gesamtbevölkerung) auf 4G-Ausrüstungen chinesischer Anbieter basierende Telekommunikationsnetze[59]. Im Oktober 2020 äußerte eine Gruppe von MdEP gegenüber den für Telekommunikation und Handel zuständigen Ministern der Mitgliedstaaten und der Kommission Bedenken, dass einer der Gründe für den großen Marktanteil chinesischer Anbieter darin bestehe, dass diese von einem unfairen wirtschaftlichen Vorteil profitierten, d. h. sie erhielten öffentliche Subventionen, die Anbietern aus der EU nach den EU-Vorschriften über staatliche Beihilfen nicht zur

[59] StrandConsult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks.

Verfügung stünden[60]. In einer kürzlich durchgeführten Analyse verwies der Hof in dieser Hinsicht auf ähnliche Risiken[61]. Solche Subventionen können den Binnenmarkt verzerren und durch die Schaffung ungleicher Wettbewerbsbedingungen für 5G-Anbieter sicherheitsrelevante Auswirkungen haben. Um dieses Problem anzugehen, schlug die Kommission im Mai 2021 eine neue Verordnung[62] vor, in der Verfahren zur Prüfung solcher Subventionen und zur Beseitigung der damit einhergehenden Marktverzerrungen festgelegt sind.

Der Kommission liegen keine ausreichenden Informationen über mögliche Substitutionskosten für Ausrüstung chinesischer Anbieter vor

79 Laut einem Bericht von Juni 2020[63] würden sich die Gesamtinvestitionskosten infolge der Beschränkungen für einen wichtigen Anbieter von 5G-Infrastrukturen in der EU in den nächsten zehn Jahren um fast 2,4 Milliarden Euro pro Jahr (d. h. 24 Milliarden Euro) erhöhen. Einer anderen Studie[64] zufolge stehen die europäischen Betreiber bereits vor der Notwendigkeit einer Modernisierung der zwischen 2012 und 2016 implementierten 4G-Netze, da es gängige Geschäftspraxis ist, Netzausrüstungen, die mehr als drei bis vier Jahre alt sind, zu überholen und zu modernisieren. Laut dieser Studie werden sich die Gesamtkosten für den Komplettaustausch nachrüstbarer Ausrüstungen, die seit 2016 von chinesischen Anbietern erworben wurden, schätzungsweise auf etwa 3 Milliarden Euro belaufen werden.

80 Der hohe Anteil von Ausrüstungen chinesischer Anbieter in Verbindung mit deren möglicher Einstufung als Hochrisikoanbieter in bestimmten Mitgliedstaaten kann zu Substitutionskosten in Milliardenhöhe führen, wenn Mobilfunknetzbetreiber die Ausrüstungen chinesischer Anbieter ohne Übergangszeit aus den europäischen Netzen entfernen und ersetzen müssen (siehe Ziffern ***77***-***79***). Grundsätzlich dürfen keine

---

[60] Schreiben der MdEP an die für Telekommunikation und Handel zuständigen Minister der EU-Mitgliedstaaten und die Kommissare Thierry Breton, Margrethe Vestager und Valdis Dombrovskis vom 14.10.2020.

[61] Analyse Nr. 03/2020 des Hofes:Die Reaktion der EU auf Chinas staatlich gelenkte Investitionsstrategie.

[62] Vorschlag für eine Verordnung über den Binnenmarkt verzerrende drittstaatliche Subventionen, COM(2021) 223 final vom 5.5.2021.

[63] Oxford Economics, Restricting competition in 5G network equipment throughout Europe, Juni 2020. (gesponsert von Huawei).

[64] StrandConsult, The real cost to 'rip and replace' Chinese equipment from telecom networks.

staatlichen Beihilfen gewährt werden, um Betreiber für die Erfüllung rechtlicher Verpflichtungen zu entschädigen, es sei denn, die Mitgliedstaaten können der Kommission Nachweise darüber vorlegen, dass die erforderlichen Voraussetzungen (z. B. ein Anreizeffekt) erfüllt sind. Bei seiner Analyse ermittelte der Hof einen Fall, in dem gemäß den nationalen Rechtsvorschriften die Möglichkeit besteht, Substitutionskosten durch nationale öffentliche Mittel zu finanzieren (siehe das finnische Gesetz über elektronische Kommunikationsdienste[65]). Die Mitgliedstaaten sind verpflichtet, der Kommission alle Fälle zu melden, in denen Mobilfunknetzbetreiber durch staatliche Beihilfen für solche Kosten entschädigt werden sollen. Nach Angaben der Kommission hat sich bislang kein Mitgliedstaat oder Interessenträger im Hinblick auf staatliche Beihilfen für Kosten für den Ersatz von Ausrüstungen mit ihr in Verbindung gesetzt. Nach Ansicht der im Rahmen der Prüfung befragten Interessenträger aus der Industrie untergraben die unklare Behandlung dieser Kosten durch die Mitgliedstaaten und mögliche Unterschiede zwischen den einzelnen Ländern die Geschäftssicherheit und könnten sich auf das Tempo der Einführung von 5G auswirken.

[65] Gesetz über elektronische Kommunikationsdienste 1207/2020 vom 30.12.2020, Artikel 301.

Schlussfolgerungen und Empfehlungen

81 Insgesamt ergab die Prüfung des Hofes, dass sich der Ausbau der 5G-Netze durch die Mitgliedstaaten trotz der Unterstützung der Kommission erheblich verzögert und weitere Anstrengungen erforderlich sind, um Sicherheitsfragen im Zusammenhang mit der 5G-Einführung anzugehen.

82 Die Kommission forderte in ihrem 5G-Aktionsplan von 2016 eine 5G-Abdeckung aller städtischen Gebiete und entlang der Hauptverkehrswege bis 2025 und im März 2021 eine vollständige Abdeckung bis 2030. Bis Ende 2020 hatten 23 Mitgliedstaaten kommerzielle 5G-Dienste eingeführt und erreichten das Zwischenziel, dass mindestens eine Großstadt Zugang zu solchen Diensten haben sollte. Die Prüfung des Hofes ergab jedoch, dass sich bei den nationalen 5G-Strategien oder -Breitbandplänen nicht alle Mitgliedstaaten an den Zielen der Kommission orientieren. Außerdem wurde in mehreren Ländern der europäische Kodex für die elektronische Kommunikation noch nicht in nationales Recht umgesetzt, und die Zuteilung von 5G-Frequenzen hat sich verzögert. Die Verzögerungen bei der Frequenzvergabe haben unterschiedliche Gründe: eine schwache Nachfrage seitens der Mobilfunknetzbetreiber, Probleme bei der grenzüberschreitenden Koordinierung mit Nicht-EU-Ländern entlang der östlichen Grenzen, die Verschiebung von Versteigerungen aufgrund der COVID-19-Pandemie und die Ungewissheit im Hinblick auf den Umgang mit Sicherheitsfragen. Angaben der Kommission zufolge werden voraussichtlich nur 11 Mitgliedstaaten das Ziel für 2025 erreichen (siehe Ziffer ***22***-***43***).

83 Die Kommission hat die Mitgliedstaaten bei der Umsetzung des 2016 verabschiedeten 5G-Aktionsplans durch Initiativen, Leitlinien und Finanzmittel für die 5G-Forschung unterstützt. Die Kommission hat jedoch nicht das erwartete Niveau der Dienstqualität der 5G-Netze festgelegt, wie etwa die Leistung in Bezug auf die Mindestgeschwindigkeit und die maximale Latenz. Dies hat die Mitgliedstaaten veranlasst, den Begriff "5G-Qualität" unterschiedlich auszulegen. Der Hof stellte fest, dass die Mitgliedstaaten unterschiedliche Ansätze für die Einführung von 5G-Diensten verfolgten; so haben beispielsweise nur zwei von ihnen eine Mindestgeschwindigkeit und eine maximale Latenz festgelegt. Letztlich besteht die Gefahr, dass diese unterschiedlichen Ansätze zu Ungleichheiten innerhalb der EU sowohl beim Zugang zu 5G-Diensten als auch bei deren Qualität führen, wodurch die "digitale Kluft" zwischen den Mitgliedstaaten und Regionen vergrößert und nicht verringert würde (siehe Ziffern ***22***-***31***).

Empfehlung 1 – Fördern einer gleichmäßigen und zügigen Einführung von 5G-Netzen in der EU

Die Kommission sollte

a) in Zusammenarbeit mit den Mitgliedstaaten eine gemeinsame Definition des erwarteten Niveaus der Dienstqualität von 5G-Netzen entwickeln, einschließlich der Leistung in Bezug auf die Mindestgeschwindigkeit und die maximale Latenz;

b) die Mitgliedstaaten auffordern, die 5G-Ziele für 2025 und 2030 und die zu ihrer Verwirklichung erforderlichen Maßnahmen in ihre Digitalisierungs- und/oder 5G-Strategien und ihre Breitbandpläne aufzunehmen, sobald diese aktualisiert werden;

c) in Bezug auf Frequenzen die Mitgliedstaaten bei der Lösung von Koordinierungsproblemen mit Nachbarländern, die nicht der EU angehören, unterstützen, z. B. durch die Forderung, das Thema auf die Tagesordnung jeder entsprechenden Sitzung zu setzen.

Zeitrahmen: Dezember 2022.

84 Die Sicherheitsaspekte im Zusammenhang mit 5G-Netzen haben sich auf EU-Ebene erst vor Kurzem zu einem wichtigen Thema entwickelt. Die daraus resultierende Notwendigkeit, auf EU-Ebene tätig zu werden, wurde 2019 vom Europäischen Rat mit seiner Forderung nach einem abgestimmten Vorgehen und einer Zusammenarbeit der Mitgliedstaaten in dieser grenzüberschreitenden Frage unterstrichen. Die Kommission hat gemeinsam mit den Mitgliedstaaten rasch auf neue Bedenken hinsichtlich der Sicherheit der 5G-Netze reagiert. Im Jahr 2020 nahm die NIS-Kooperationsgruppe ein EU-Instrumentarium für die 5G-Cybersicherheit an, in dem verschiedene strategische, technische und unterstützende Maßnahmen zur Bewältigung von Bedrohungen für die Sicherheit von 5G-Netzen aufgeführt und für jede dieser Maßnahmen die zuständigen Akteure benannt werden. Mehrere davon betreffen 5G-Hochrisikoanbieter. Dieses Instrumentarium wurde anschließend von der Kommission und dem Europäischen Rat gebilligt (siehe Ziffern ***45***-***47***). Da es sich jedoch um ein Soft-Law-Instrument handelt, sind diese Maßnahmen daher für die Mitgliedstaaten nicht bindend. In jüngerer Zeit wurde das EU-Instrumentarium für die 5G-Cybersicherheit in der neuen europäischen Strategie zur Förderung intelligenter, sauberer und sicherer Verbindungen in digitalen Systemen in der ganzen Welt als Instrument zur Lenkung von Investitionen in digitale Infrastruktur erwähnt (siehe Ziffer ***50***).

85 Die in dem Instrumentarium festgelegten Kriterien bieten einen operativen Rahmen, der für die koordinierte Bewertung des Risikoprofils der Anbieter in allen Mitgliedstaaten hilfreich ist. Gleichzeitig sind für die Durchführung dieser Bewertung nach wie vor die Mitgliedstaaten zuständig (siehe Ziffer ***54***).

86 Seit der Annahme des Instrumentariums wurden bei der Erhöhung der Sicherheit von 5G-Netzen Fortschritte erzielt, wobei die meisten Mitgliedstaaten Hochrisikoanbietern Beschränkungen auferlegt haben oder dabei sind, dies zu tun. Bis Oktober 2021 hatten 13 Mitgliedstaaten unter Berücksichtigung dieses Rahmens ihre Rechtsvorschriften zur 5G-Sicherheit in Kraft gesetzt oder geändert. Weitere Mitgliedstaaten werden in Kürze Rechtsvorschriften vorlegen, die den Kriterien des Instrumentariums Rechnung tragen (siehe Ziffern ***54*** und ***75***).

87 Das Instrumentarium wurde zwar in einer frühen Phase der 5G-Einführung angenommen, aber eine Reihe von Mobilfunknetzbetreibern hatte ihre Anbieter bereits ausgewählt (siehe Ziffer ***52***). Die Nichtberücksichtigung von Sicherheitsfragen bei der Gestaltung der Politik könnte sich negativ auf die Umsetzung auswirken; so könnte der erwartete Nutzen (z. B. das BIP-Wachstum) durch die Kosten für die Abwehr von Bedrohungen, insbesondere im Zusammenhang mit Cyberkriminalität, untergraben werden (siehe Ziffern ***02*** und ***04***).

88 Das Instrumentarium trägt den nationalen Zuständigkeiten und den landesspezifischen Faktoren Rechnung. Die Prüfung des Hofes ergab, dass die Mitgliedstaaten bisher unterschiedliche Ansätze in Bezug auf die Verwendung von Ausrüstung von Hochrisikoanbietern oder den Umfang der Beschränkungen verfolgen (z. B. Beschränkung auf kritische Komponenten oder Komponenten des 5G-Kernnetzes oder Berücksichtigung des gesamten oder eines Teils des Funkzugangsnetzes) (siehe Ziffern ***74*** und ***75***).

89 In den kommenden Jahren könnten die Gesetze zur 5G-Sicherheit, die von den Mitgliedstaaten auf der Grundlage des Instrumentariums erlassen werden, zu einheitlicheren Ansätzen gegenüber 5G-Hochrisikoanbietern führen. Da jedoch keine der in diesem Instrumentarium angeführten Maßnahmen rechtlich bindend ist, hat die Kommission keine Handhabe, um sie durchzusetzen. Daher besteht nach wie vor die Gefahr, dass das Instrumentarium als solches nicht gewährleisten kann, dass die Mitgliedstaaten in Fragen der Netzsicherheit in abgestimmter Weise vorgehen (siehe Ziffern ***49***-***75***).

90 Viele 5G-Anbieter sind außerhalb der EU niedergelassen, was bedeutet, dass ihr Betrieb durch Rechtsvorschriften von Drittländern geregelt wird. Diese sind mitunter sehr weit von den EU-Standards entfernt, z. B. im Hinblick auf die Wirksamkeit des den Bürgerinnen und Bürgern gewährten Datenschutzes oder allgemein in Bezug darauf, wie die Unabhängigkeit der Justiz durch ein System gesetzgeberischer und demokratisch legitimierter Kontroll- und Einflussrechte gewährleistet wird. Dass 5G-Netze überwiegend auf Software-Anwendungen beruhen, könnte ebenfalls in besonderem Maße Anlass zur Besorgnis geben, wenn die Zentren zur Kontrolle dieser Software in Nicht-EU-Ländern ansässig sind und Unionsbürgerinnen und -bürger daher möglicherweise Rechtsvorschriften von Drittländern unterliegen. Die Kommission hat erste Schritte unternommen, um auf diese Bedenken einzugehen, indem sie feststellte, dass jedes Unternehmen, das Dienstleistungen für die europäischen Bürgerinnen und Bürger erbringt, die EU-Vorschriften und -Werte einhalten muss. Außerdem ist sie mit mehreren Ländern in einen Dialog getreten, um ein hohes Maß an Schutz der Vertraulichkeit personenbezogener Daten zu gewährleisten (siehe Ziffern ***56***-***62***).

91 Obwohl die Bedenken hinsichtlich der 5G-Sicherheit von Natur aus grenzübergreifend sind, liegen der Öffentlichkeit insgesamt kaum Informationen darüber vor, wie die Mitgliedstaaten Sicherheitsfragen angehen, insbesondere was Hochrisikoanbieter betrifft. Die Kommission überwacht die Fortschritte bei der Umsetzung des Instrumentariums und erstattet darüber Bericht. Die Berichte enthalten jedoch keine detaillierten und vergleichbaren Informationen darüber, wie die Mitgliedstaaten Fragen im Zusammenhang mit der Sicherheit der 5G-Netze behandeln. Bis September 2021 gab es zudem keine Pläne für weitere Berichte. Dieser Mangel an Informationen erschwert den Wissensaustausch zwischen den Mitgliedstaaten und die Möglichkeit, abgestimmte Maßnahmen durchzuführen. Ferner begrenzt dies den Spielraum der Kommission, Vorschläge zur Verbesserung der Sicherheit der 5G-Netze zu unterbreiten (siehe Ziffern ***68***-***73***).

Empfehlung 2 – Ein abgestimmtes Vorgehen der Mitgliedstaaten in Bezug auf die 5G-Sicherheit unterstützen

Die Kommission sollte

a) weitere Orientierungshilfen oder Unterstützungsmaßnahmen zu Schlüsselelementen des EU-Instrumentariums bereitstellen, z. B. Kriterien für die Bewertung von 5G-Anbietern und deren Einstufung als Hochrisikoanbieter sowie Datenschutzerwägungen.

Zeitrahmen: Dezember 2022.

b) die Transparenz hinsichtlich der Ansätze der Mitgliedstaaten für die Sicherheit der 5G-Netze fördern, insbesondere durch Überwachung und Berichterstattung über die Umsetzung der Sicherheitsmaßnahmen des EU-Instrumentariums für die 5G-Cybersicherheit. Zu diesem Zweck sollten gemeinsame zentrale Leistungsindikatoren verwendet werden.

Zeitrahmen: Dezember 2022.

c) gemeinsam mit den Mitgliedstaaten bewerten, welche Aspekte der Sicherheit von 5G-Netzen durchsetzbare Anforderungen erfordern, und gegebenenfalls entsprechende Rechtsvorschriften auf den Weg bringen.

Zeitrahmen: Dezember 2022.

92 Die Kommission hat damit begonnen, sich mit den damit verbundenen Vorwürfen der Erlangung eines unlauteren wirtschaftlichen Vorteils durch ausländische Subventionen zu befassen. Solche Subventionen können den Binnenmarkt verzerren, ungleiche Wettbewerbsbedingungen für 5G-Anbieter schaffen und sich auf die Sicherheit auswirken (siehe Ziffer ***78***).

93 Was den Umgang mit möglichen Substitutionskosten durch die Mitgliedstaaten angeht, die entstehen könnten, wenn Mobilfunknetzbetreiber Ausrüstung von Hochrisikoanbietern ohne Übergangszeit aus den EU-Netzen entfernen müssen, verfügt die Kommission nicht über ausreichende Informationen. Eine unterschiedliche Behandlung könnte die Geschäftssicherheit untergraben und sich auf das Tempo der 5G-Einführung auswirken (siehe Ziffern ***79*** und ***80***). Darüber hinaus können unterschiedliche Ansätze der Mitgliedstaaten hinsichtlich der Sicherheit von 5G-Netzen und insbesondere das Fehlen eines abgestimmten Vorgehens auf EU-Ebene das reibungslose Funktionieren des Binnenmarkts beeinträchtigen. Bisher hat die Kommission dazu keine Bewertung vorgenommen (siehe Ziffern ***74***-***76***).

Empfehlung 3 – Die 5G-Sicherheitskonzepte der Mitgliedstaaten überwachen und die Auswirkungen von Divergenzen auf das wirksame Funktionieren des Binnenmarkts bewerten

Die Kommission sollte

a) einen transparenten und kohärenten Ansatz für den Umgang der Mitgliedstaaten mit den Kosten fördern, die den Mobilfunknetzbetreibern beim Austausch von 5G-Ausrüstung entstehen, die von Hochrisikoanbietern bezogen wurde, indem sie eine Überwachung und regelmäßige Berichterstattung im Rahmen der Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit gewährleistet;

b) bewerten, wie sich der Aufbau eines 5G-Netzes durch einen Mitgliedstaat mit Ausrüstung, die von einem Anbieter erworben wurde, der in einem anderen Mitgliedstaat als Hochrisikoanbieter eingestuft ist, auf den Binnenmarkt auswirken würde.

Zeitrahmen: Dezember 2022.

Dieser Bericht wurde von Kammer II unter Vorsitz von Frau Iliana Ivanova, Mitglied des Rechnungshofs, am 15. Dezember 2021 in Luxemburg angenommen.

Für den Rechnungshof

Klaus-Heiner LEHNE
Präsident

Anhänge

Anhang I – Wichtige Chancen und Risiken bei 5G

Quelle: Europäischer Rechnungshof, auf der Grundlage von Informationen des Wissenschaftlichen Dienstes des Europäischen Parlaments – Europäisches Wissenschaftsmedienzentrum.

Anhang II – Beispiele für Auswirkungen von Störungen von Telekommunikationsnetzen und Cybersicherheitsvorfällen

Ausfall der Notrufnummern in Frankreich[66,67]

01 Am 3. Juni 2021 hat ein Netzausfall bei Orange, dem größten französischen Telekommunikationsbetreiber, zu einem Ausfall der Notrufdienste geführt, der mehrere Stunden anhielt. Während ein Cyberangriff als Ursache ausgeschlossen wurde, zeigt dieser Vorfall, welche Auswirkungen die Störung einer kritischen Netzinfrastruktur haben kann.

Ransomware-Angriffe auf den irischen öffentlichen Gesundheitsdienst[68,69,70]

02 Im Mai 2021 schaltete der irische Gesundheitsdienst (Health Service Executive) aufgrund eines Ransomware-Angriffs alle seine IT-Systeme ab. Von dem Angriff waren alle Aspekte der Patientenversorgung betroffen, da er den Zugang zu Patientenakten erschwerte und das Risiko für Verzögerungen und Fehler erhöhte. Zwar haben die irischen Beamten keine Kenntnis von einer Gefährdung von Patientendaten, die Weitergabe von Patientenakten hätte aber zu allen Arten von damit zusammenhängenden Straftaten führen können, wie etwa Betrug und Erpressung. Nach Angaben des Generaldirektors des Gesundheitsdienstes werden die Kosten der Wiederherstellung der Systemintegrität auf 500 Millionen Euro (600 Millionen US-Dollar) geschätzt.

---

66 https://www.euronews.com/2021/06/03/french-telecom-operator-orange-apologises-after-emergency-numbers-crash-nationwide

67 https://www.reuters.com/business/media-telecom/orange-blames-network-outage-software-failure-audit-2021-06-11/

68 https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875

69 https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

70 https://www.cert.europa.eu/cert/moreclusteredition/en/blog_DataBreachTodayinRSSSyndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds[71,72,73]

03 Solarwinds ist ein US-amerikanisches Unternehmen, das Software für die Verwaltung von Computernetzen, -systemen und -infrastrukturen für Unternehmen sowie staatliche und föderale Behörden entwickelt. Anfang 2020 war Solarwinds Ziel eines Software-Angriffs. Den Piraten gelang es, die Angriffe auf die Kunden von Solarwinds über Software-Updates zu führen, die Schadcodes enthielten. Diese öffneten eine Hintertür zu den Kundenplattformen und ermöglichten so einen einfachen Zugang für Angriffe und die Installation weiterer Schad- und Spähsoftware.

[71] https://www.solarwinds.com/

[72] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[73] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

Anhang III – Rechtlicher und politischer Rahmen

Europäische Kommission

Europäischer Rat / Rat der Europäischen Union

Rechtsvorschriften

NIS-Kooperationsgruppe

2016 – NIS-Richtlinie, Juli 2016 – Einführung rechtlicher Maßnahmen zur Verbesserung des Gesamtniveaus der Cybersicherheit in der Union.

2016 – 5G-Aktionsplan, September 2016 – Ziel der Einführung von 5G-Diensten in allen Mitgliedstaaten bis 2020 und zügiger Ausbau, um bis 2025 eine nahtlose 5G-Versorgung in städtischen Gebieten und entlang der wichtigsten Verkehrsachsen zu gewährleisten.

2018 – Kodex für die elektronische Kommunikation, Dezember 2018 – Ziel der Verwirklichung eines Binnenmarktes für elektronische Kommunikationsnetze und -dienste.

2019 – Schlussfolgerungen des Rates, März 2019 – Der Europäische Rat sieht der Empfehlung der Kommission zu einem abgestimmten Vorgehen bei der Sicherheit von 5G-Netzen erwartungsvoll entgegen.

2019 – Empfehlung "Cybersicherheit der 5G-Netze, März 2019 – Die Kommission empfiehlt den Mitgliedstaaten, die Cybersicherheitsrisiken, die 5G-Netze auf nationaler Ebene betreffen, zu bewerten und die erforderlichen Sicherheitsmaßnahmen zu ergreifen.

2019 – Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft, Dezember 2019 – Der Rat hebt hervor, dass ein zügiger und sicherer Ausbau der 5G-Netze eine zentrale Voraussetzung für die Verbesserung der Wettbewerbsfähigkeit der EU ist und einen abgestimmten Ansatz in der EU erfordert.

2020 – EU-Instrumentarium für die 5G-Cybersicherheit, Januar 2020 – Ermittlung eines möglichen gemeinsamen Maßnahmenpakets zur Minderung der wichtigsten Cybersicherheitsrisiken im Zusammenhang mit 5G-Netzen.

2020 – Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums, Januar 2020 – Die Europäische Kommission billigt das Instrumentarium und legt die nächsten Schritte fest (z. B. Erstellung eines Berichts über den Stand der Umsetzung bis Juni 2020).

2020 – Schlussfolgerungen des Rates zur Gestaltung der digitalen Zukunft Europas, Juni 2020 – Der Rat stimmt der Auffassung zu, dass ein koordinierter Ansatz zur Eindämmung der Hauptrisiken für eine sichere 5G-Einführung in der EU gewährleistet und umgesetzt werden muss.

2020 – Schlussfolgerungen des Rates, Oktober 2020 – Der Rat billigt das EU-Instrumentarium für die 5G-Cybersicherheit, insbesondere hinsichtlich der Anwendung der einschlägigen Beschränkungen für Hochrisikoanbieter.

2020 – Empfehlung [...] zur Gewährleistung eines [...] Zugangs zu 5G-Funkfrequenzen, September 2020- – Die Empfehlung enthält Leitlinien für die Entwicklung bewährter Verfahren zur Förderung der Konnektivität und zur Gewährleistung eines raschen und investitionsfreundlichen Zugangs zu 5G-Funkfrequenzen.

2020 – Die Cybersicherheitsstrategie der EU für die digitale Dekade, Dezember 2020 – Ein "Soft Law"-Dokument, in dem die Prioritäten der Kommission und die geplanten Maßnahmen im Bereich der Cybersicherheit insgesamt, einschließlich der 5G-Netze, dargelegt sind.

2020 – Vorschlag für eine NIS 2-Richtlinie, Dezember 2020 – Ziel der Modernisierung und Ausweitung des Anwendungsbereichs der bisherigen Richtlinie auf die Cybersicherheit von 5G-Netzen.

2020 – Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen, Dezember 2020 – Ziel der Verringerung von Schwachstellen bei kritischen Infrastrukturen, die für das Funktionieren der Gesellschaften und Wirtschaft der EU unerlässlich sind.

2020 – Digitaler Kompass 2030: der europäische Weg in die digitale Dekade, März 2021 – Aufzeigen eines Weges zu einer gemeinsamen Vision und Maßnahmen, die Europa in die Lage versetzen, die Ziele der digitalen Dekade zu erreichen.

2021 – Schlussfolgerungen des Rates zur Cybersicherheitsstrategie der EU für die digitale Dekade, März 2021 – Unterstützung der nächsten Schritte zur Cybersicherheit von 5G-Netzen, wie sie in der Anlage zur Cybersicherheitsstrategie der EU dargelegt werden.

Anhang IV – Beispiele für aus dem EFSI kofinanzierte Projekte

EFSI-Finanzierung von Projekten mit 5G-Bezug

Die beiden aus dem EFSI geförderten Projekte, die Gegenstand der Analyse des Hofes waren, betrafen Investitionen in Forschung, Entwicklung und Innovation, um die Produktpalette für 5G-Netze zu erweitern. Dabei ging es um die Entwicklung von Hardware und Software für das Funkzugangsnetz und das Kernnetz. Beide Projekte trugen zu einem engmaschigeren Funkzellennetz bei, unterstützten die Normung und erleichterten die Erprobung von Schlüsseltechnologien.

Die Projekte wurden 2018 begonnen und im Dezember 2020 abgeschlossen. Insgesamt beliefen sich die Investitionskosten auf insgesamt 3,9 Milliarden Euro, davon 1 Milliarde Euro aus dem EFSI.

Anhang V – Beispiele für im Rahmen von Horizont 2020 und aus dem EFRE geförderte Projekte

Projekt mit 5G-Bezug im Rahmen von Horizont 2020

Im Rahmen dieses Projekts werden Ausrüstungen der drei größten 5G-Anbieter (Ericsson, Huawei und Nokia) eingesetzt, um die 5G-Technologien im grenzüberschreitenden Korridor zwischen den Städten Metz (Frankreich), Merzig (Deutschland) und Luxemburg zu erproben. Das Projekt begann im November 2018 und die geplante Laufzeit betrug 31 Monate. Die EU stellte 12,9 Millionen Euro von den insgesamt veranschlagten 17,1 Millionen Euro bereit.

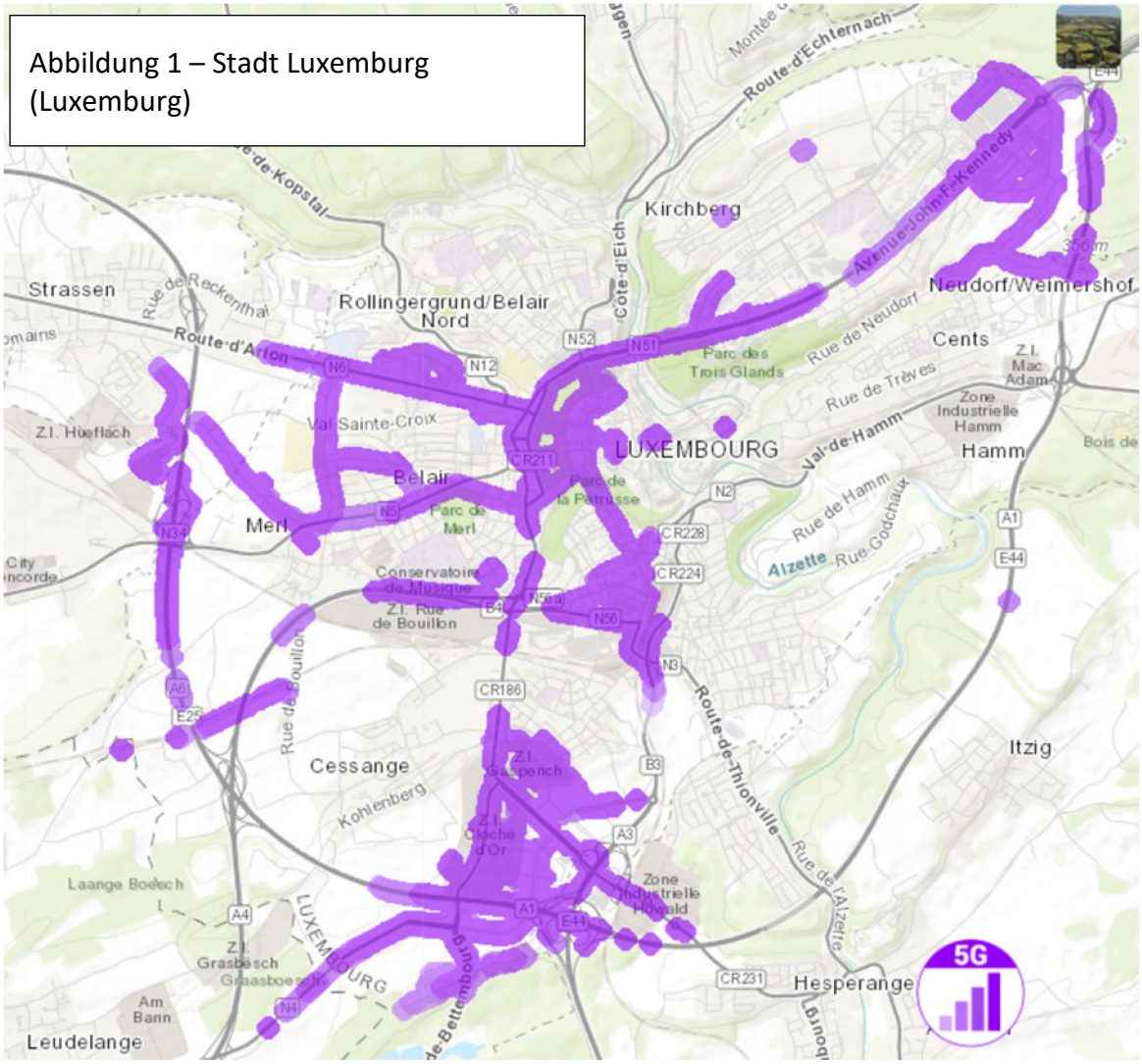
EFRE-Finanzierung eines Projekts mit 5G-Bezug

Ziel dieses in Spanien durchgeführten Projekts ist die Bereitstellung von Informationen über den Ausbau von 5G-Netzen. Dazu gehören unter anderem die Erprobung von Netzmanagementtechniken, die durch die 5G-Technologie ermöglicht werden, wie Netzvirtualisierung, Edge Computing, die dynamische Zuweisung von Netzressourcen und Network Slicing sowie die Entwicklung von 5G-Anwendungen. Das Projekt begann 2019 und die geplante Laufzeit betrug 30 Monate. Von den veranschlagten Gesamtkosten in Höhe von 7,1 Millionen Euro leistete die EU einen Beitrag in Höhe von 2,2 Millionen Euro.

Anhang VI – 5G-Abdeckung in ausgewählten Städten

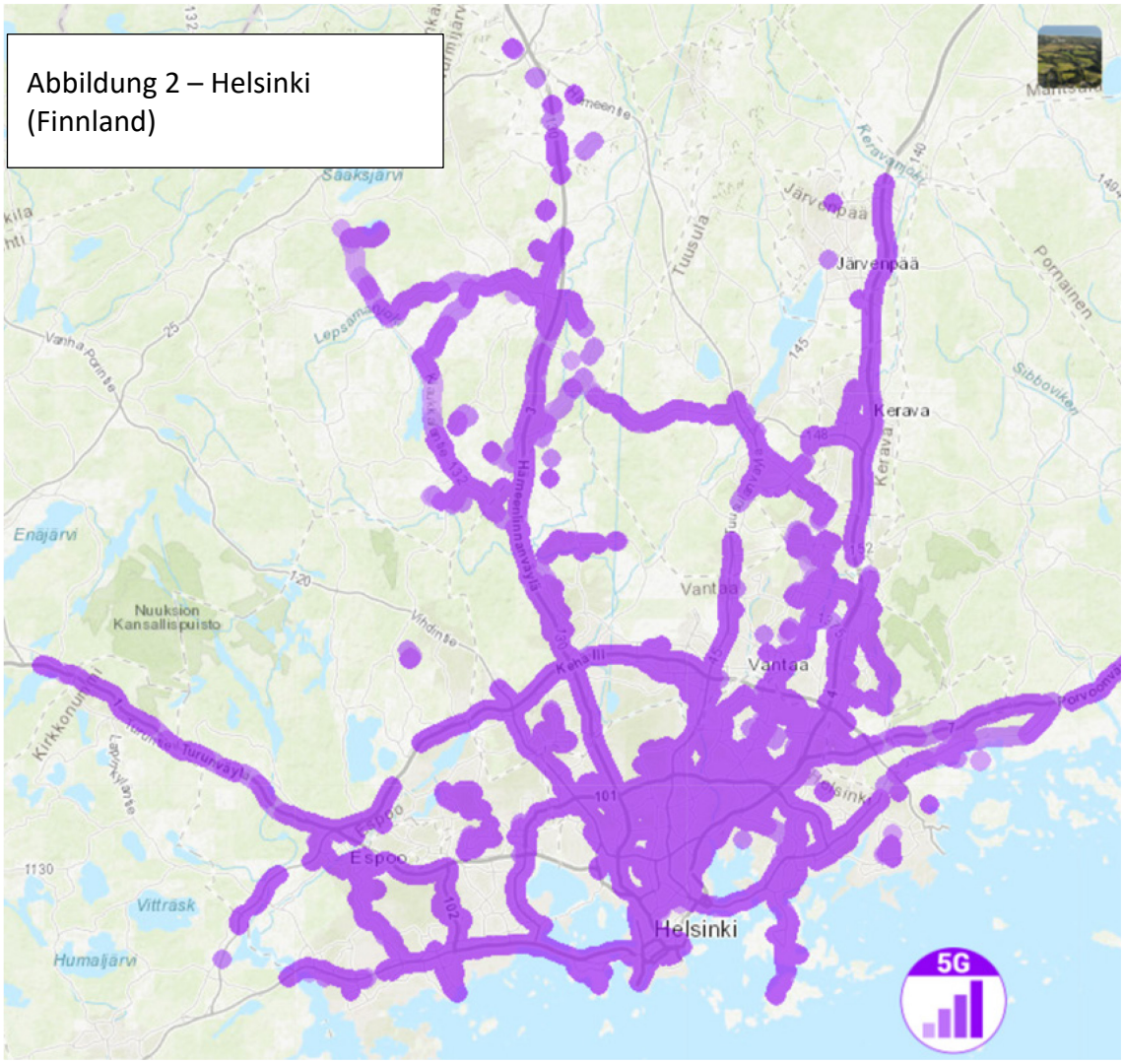
Die folgenden Zahlen beruhen auf Daten über mobile Breitbandverbindungen, die über Tests von Nutzern der App Nperf erfasst wurden. Die Gebiete, in denen 5G-Signale erkannt wurden, sind nicht unbedingt für die kommerzielle Nutzung freigegeben. Da die Netzleistung von einem Mobilfunknetzbetreiber zum anderen unterschiedlich ist, zeigen die folgenden Karten, die am 4. Oktober 2021 extrahiert wurden, nur die Abdeckung, nicht aber die Leistung, die sich durch Geschwindigkeit und Latenz auszeichnet.

Abbildung 1 – Stadt Luxemburg (Luxemburg)



© nPerf.

Abbildung 2 – Helsinki (Finnland)



© nPerf.

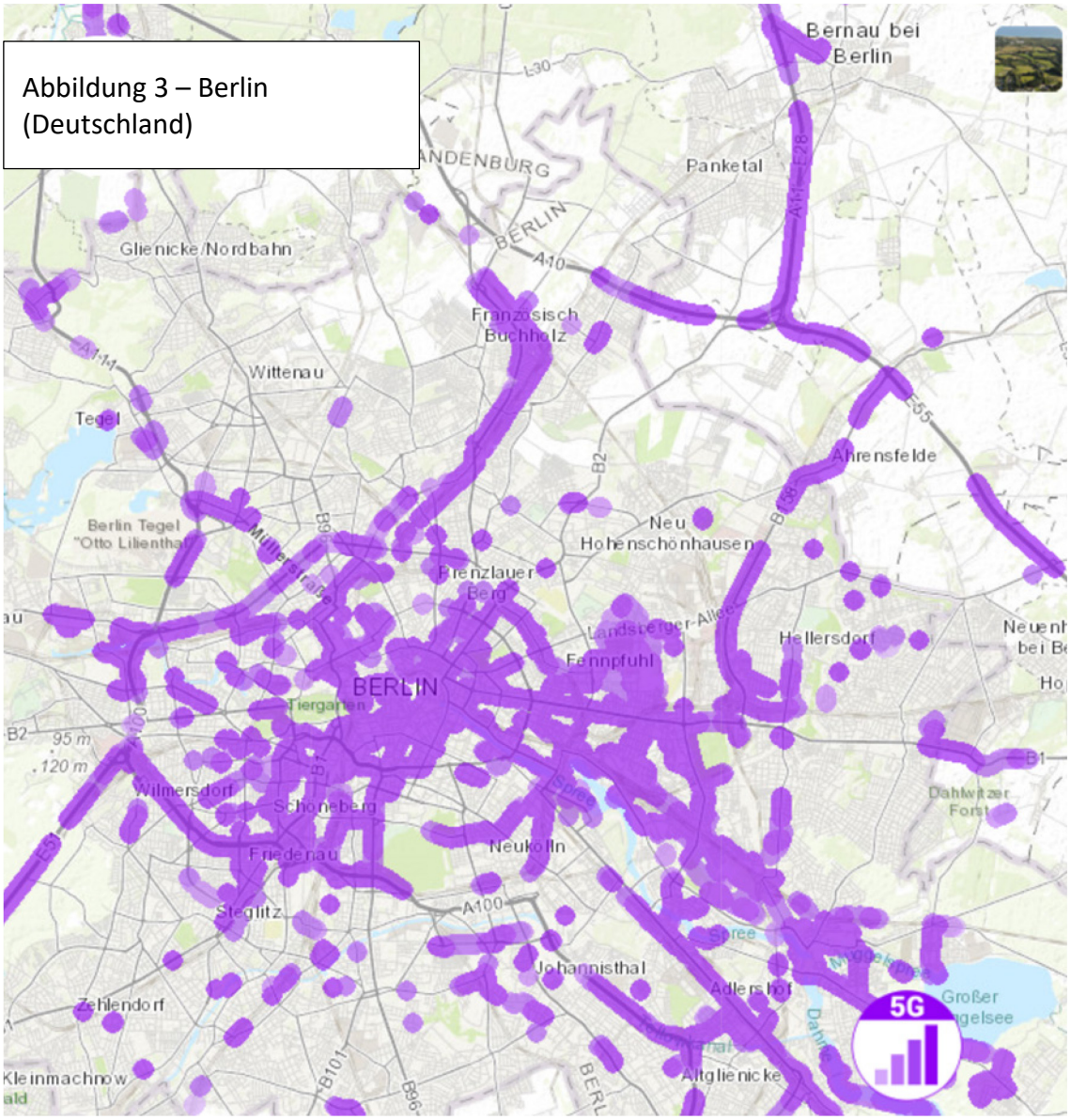


Abbildung 3 – Berlin (Deutschland)

© nPerf.

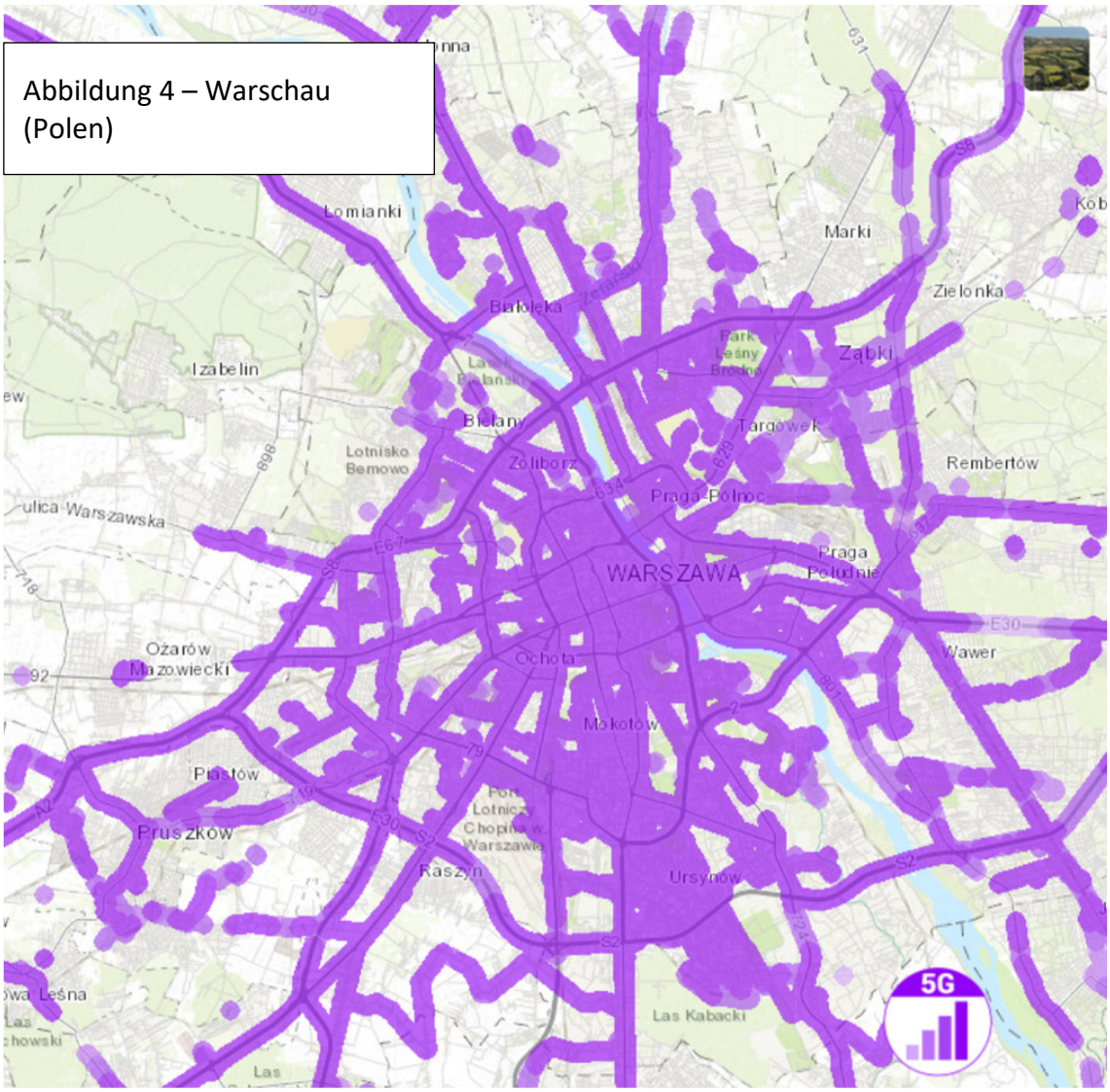


Abbildung 4 – Warschau (Polen)

© nPerf.

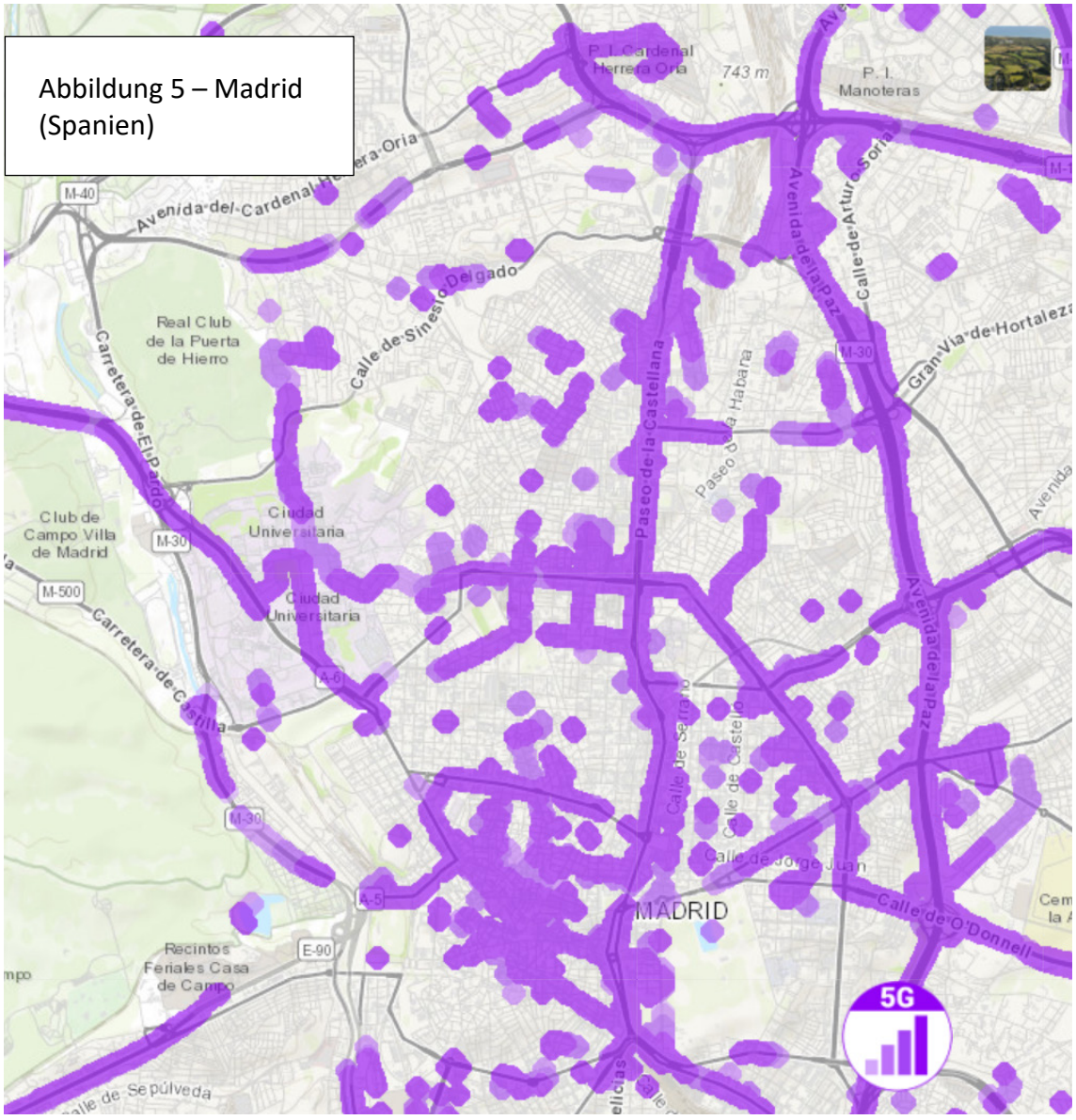


Abbildung 5 – Madrid (Spanien)

© nPerf.

Anhang VII – EU-Instrumentarium für die 5G-Cybersicherheit

Das von der NIS-Kooperationsgruppe angenommene und von der Kommission gebilligte EU-Instrumentarium für die 5G-Cybersicherheit umfasst drei Arten nicht verbindlicher Maßnahmen (strategische, technische und Unterstützungsmaßnahmen), die von verschiedenen Akteuren durchgeführt werden müssen (siehe nachstehende Zusammenfassung).

Einzelmaßnahmen	Relevante Akteure				
	Behörden der Mitgliedstaaten	Mobilfunknetz-betreiber	Europäische Kommission	ENISA	Interessenträger (einschl. Anbietern)
Strategische Maßnahmen					
SM01 – Stärkung der Rolle der nationalen Behörden	✓	✓			
SM02 – Durchführung von Prüfungen bei den Betreibern und Anforderung von Informationen	✓	✓			
SM03 – Analyse des Risikoprofils der Anbieter und Anwendung von Beschränkungen auf Anbieter, die mit Blick auf wichtige Anlagen und Einrichtungen als Hochrisikoanbieter eingestuft wurden, einschließlich der für eine wirksame Risikominderung erforderlichen Ausschlüsse	✓	✓			
SM04 – Kontrolle des Einsatzes von Anbietern verwalteter Dienstleistungen (Managed Service Providers) und der Third-line-Wartung der Ausrüstungsanbieter	✓	✓			
SM05 – Gewährleistung der Anbietervielfalt für die verschiedenen Mobilfunknetzbetreiber durch geeignete Strategien bei Nutzung mehrerer Anbieter	✓	✓			
SM06 – Stärkung der Resilienz auf nationaler Ebene	✓	✓			
SM07 – Ermittlung wichtiger Anlagen und Einrichtungen und Förderung eines diversifizierten und nachhaltigen 5G-Ökosystems in der EU	✓		✓		
SM08 – Aufrechterhaltung und Stärkung der Vielfalt und der Kapazitäten der EU in Bezug auf die Netztechnologien der Zukunft	✓		✓		✓
Technische Maßnahmen					
TM01 – Gewährleistung der Anwendung grundlegender Sicherheitsanforderungen (Sicherheit von Netzdesign und -architektur)	✓	✓			

Einzelmaßnahmen	Relevante Akteure				
	Behörden der Mitgliedstaaten	Mobilfunknetz-betreiber	Europäische Kommission	ENISA	Interessenträger (einschl. Anbietern)
TM02 – Gewährleistung und Bewertung der Umsetzung von Sicherheitsmaßnahmen bei bestehenden 5G-Standards	✓	✓			✓
TM03 – Gewährleistung strenger Zugangskontrollen	✓	✓			
TM04 – Erhöhung der Sicherheit virtualisierter Netzfunktionen	✓	✓			
TM05 – Gewährleistung der Sicherheit von Verwaltung, Betrieb und Überwachung der 5G-Netze	✓	✓			
TM06 – Verbesserung der physischen Sicherheit	✓	✓			
TM07 – Verbesserung der Softwareintegrität sowie des Update- und Patch-Managements	✓	✓			
TM08 – Erhöhung der Sicherheitsstandards für Anbieterprozesse durch Festlegung strenger Beschaffungsbedingungen	✓	✓			✓
TM09 – Anwendung der EU-Zertifizierung auf 5G-Netzkomponenten, Kundenausrüstung und/oder Anbieterprozesse	✓	✓	✓	✓	✓
TM10 – Nutzung der EU-Zertifizierung für andere nicht 5G-spezifische IKT-Produkte und -Dienste (vernetzte Geräte, Cloud-Dienste)	✓		✓	✓	✓
TM11 – Stärkung der Resilienz- und Betriebskontinuitätspläne	✓	✓			✓
Unterstützungsmaßnahmen					
SA01 – Überprüfung oder Entwicklung von Leitlinien und bewährten Verfahren im Bereich der Netzsicherheit	✓	✓		✓	
SA02 – Stärkung der Test- und Prüfkapazitäten auf nationaler und EU-Ebene	✓		✓	✓	
SA03 – Unterstützung und Gestaltung der 5G-Normung	✓	✓	✓	✓	✓
SA04 – Ausarbeitung von Leitlinien für die Integration von Sicherheitsmaßnahmen in bestehende 5G-Normen	✓			✓	
SA05 – Gewährleistung der Anwendung standardisierter technischer und organisatorischer Sicherheitsmaßnahmen durch ein spezielles europäisches Zertifizierungsschema	✓			✓	✓
SA06 – Austausch bewährter Verfahren bei der Umsetzung strategischer Maßnahmen, insbesondere nationaler Rahmen für die Bewertung des Risikoprofils der Anbieter	✓				

Einzelmaßnahmen	Relevante Akteure				
	Behörden der Mitgliedstaaten	Mobilfunknetz-betreiber	Europäische Kommission	ENISA	Interessenträger (einschl. Anbietern)
SA07 – Verbesserung der Koordinierung der Reaktion bei Sicherheitsvorfällen und des Krisenmanagements	✓			✓	
SA08 – Durchführung von Prüfungen der Interdependenzen zwischen 5G-Netzen und anderen kritischen Diensten	✓				
SA09 – Stärkung der Mechanismen für Zusammenarbeit, Koordinierung und Informationsaustausch	✓			✓	
SA10 – Gewährleistung der Berücksichtigung von Cybersicherheitsrisiken in mit öffentlichen Mitteln finanzierten 5G-Projekten	✓		✓		

Quelle: EU-Instrumentarium für die 5G-Cybersicherheit.

Akronyme und Abkürzungen

BIP: Bruttoinlandsprodukt

EECC: *European Electronic Communications Code* (Europäischer Kodex für die elektronische Kommunikation)

EFRE: Europäischer Fonds für regionale Entwicklung

EFSI: Europäischer Fonds für strategische Investitionen

EIB: Europäische Investitionsbank

ENISA: *European Union Agency for Cybersecurity* (Agentur der Europäischen Union für Cybersicherheit)

GEREK: Gremium Europäischer Regulierungsstellen für elektronische Kommunikation

NBP: Nationaler Breitbandplan

NIS: Netz- und Informationssystem

RAN: *Radio access network* (Funkzugangsnetz)

Glossar

Agentur der Europäischen Union für Cybersicherheit EU-Agentur zur Entwicklung und Aufrechterhaltung eines hohen Niveaus der Netz- und Informationssicherheit in allen Bereichen des privaten und öffentlichen Lebens.

Breitband: gleichzeitige Übertragung von Informationen in verschiedenen Formaten (z. B. Daten, Sprache und Video) mit hoher Geschwindigkeit.

Europäischer Fonds für strategische Investitionen: von der Europäischen Investitionsbank (EIB) und der Kommission im Rahmen der Investitionsoffensive für Europa eingeführter Mechanismus zur Förderung von Investitionen, mit dem bei Projekten von strategischer Bedeutung für die EU private Mittel eingeworben werden sollen.

Exabyte: Maßeinheit der digitalen Datenspeicherkapazität, die 1 Milliarde Gigabyte entspricht.

Funkfrequenzspektrum: der Teil des elektromagnetischen Spektrums, in dem die Funkfrequenzen liegen.

Funkzugangsnetz: wichtiger Bestandteil der modernen Telekommunikationstechnologie, der einzelne Geräte über Funk mit anderen Teilen eines Netzes verbindet.

***Global System for Mobile Communications Association* (GSMA):** Industrieverband, der weltweit die Interessen von Mobilfunknetzbetreibern sowie von Hersteller- und Dienstleistungsunternehmen und Organisationen mit Interesse an Mobilfunkinfrastrukturen vertritt.

Gremium Europäischer Regulierungsstellen für elektronische Kommunikation: eine aus Vertretern der nationalen Regulierungsbehörden der Mitgliedstaaten bestehende Einrichtung, die diese Behörden und die Kommission bei der Umsetzung des EU-Rechtsrahmens zur Schaffung eines Binnenmarkts für elektronische Kommunikation unterstützt.

Gruppe für Frequenzpolitik: hochrangige Beratergruppe, die mit Vertretern der Mitgliedstaaten besetzt ist und die EU-Institutionen bei der Entwicklung des Binnenmarktes für drahtlose Produkte und Dienste unterstützt und berät.

Internet der Dinge: Gegenstände, die mit Sensoren, Software und anderen Technologien ausgerüstet sind, mit denen sie sich über Funk verbinden und Daten mit anderen Geräten und Systemen austauschen können.

Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe): Gremium, das durch die NIS-Richtlinie eingerichtet wurde, um die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten sicherzustellen. Es setzt sich aus Vertretern der EU-Mitgliedstaaten, der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit zusammen.

Latenz: in Computernetzen die Zeit, die ein Datensatz für die Übertragung zwischen zwei Punkten benötigt.

Mobilfunknetzbetreiber: Telekommunikationsunternehmen, das angemeldeten Mobiltelefonbenutzern drahtlose Sprach- und Datenkommunikation ermöglicht.

Nationaler Breitbandplan: Dokument der Mitgliedstaaten, das strategische Zielen im Hinblick auf die Verwirklichung der Breitbandziele der EU enthält.

Ransomware: Schadprogramm, das den Opfern den Zugang zu einem Computersystem verwehrt oder Dateien unlesbar macht und das Opfer zwingt, ein Lösegeld zu zahlen, damit der Zugang wiederhergestellt wird.

Antworten der Kommission

https://www.eca.europa.eu/de/Pages/DocItem.aspx?did=60614

Zeitschiene

https://www.eca.europa.eu/de/Pages/DocItem.aspx?did=60614

Prüfungsteam

Die Sonderberichte des Hofes enthalten die Ergebnisse seiner Prüfungen zu Politikbereichen und Programmen der Europäischen Union oder zu Fragen des Finanzmanagements in spezifischen Haushaltsbereichen. Bei der Auswahl und Gestaltung dieser Prüfungsaufgaben ist der Hof darauf bedacht, maximale Wirkung dadurch zu erzielen, dass er die Risiken für die Wirtschaftlichkeit oder Regelkonformität, die Höhe der betreffenden Einnahmen oder Ausgaben und künftige Entwicklungen sowie das politische und öffentliche Interesse abwägt.

Diese Wirtschaftlichkeitsprüfung wurde von Prüfungskammer II – Ausgabenbereich "Investitionen für Kohäsion, Wachstum und Integration" – unter Vorsitz von Iliana Ivanova, Mitglied des Hofes, durchgeführt. Die Prüfung stand unter der Leitung von Annemie Turtelboom, Mitglied des Hofes. Frau Turtelboom wurde unterstützt von ihrer Kabinettchefin Florence Fornaroli und dem Attaché Celil Ishik, dem Leitenden Manager Niels-Erik Brokopp, dem Aufgabenleiter Paolo Pesce sowie den Prüferinnen und Prüfern Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov und Nils Westphal.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7406-7	ISSN 1977-5644	doi:10.2865/920436	QJ-AB-21-029-DE-N
HTML	ISBN 978-92-847-7392-3	ISSN 1977-5644	doi:10.2865/502016	QJ-AB-21-029-DE-Q

Schätzungen zufolge wird das europäische BIP durch 5G zwischen 2021 und 2025 um bis zu 1 Billion Euro wachsen. Infolgedessen könnten bis zu 20 Millionen Arbeitsplätze in sämtlichen Bereichen der Wirtschaft neu geschaffen oder umgewandelt werden. Der Hof stellte fest, dass Verzögerungen die Verwirklichung der EU-Ziele für die 5G-Einführung gefährden und weitere Anstrengungen erforderlich sind, um Sicherheitsprobleme zu bewältigen. In dem Bericht unterbreitet der Hof der Kommission eine Reihe von Empfehlungen, die darauf abstellen, den zügigen und aufeinander abgestimmten Auf- und Ausbau sicherer 5G-Netze in der EU voranzutreiben.

Sonderbericht des Hofes gemäß Artikel 287 Absatz 4 Unterabsatz 2 AEUV.

EUROPÄISCHER RECHNUNGSHOF

Amt für Veröffentlichungen der Europäischen Union

EUROPÄISCHER RECHNUNGSHOF
12, rue Alcide De Gasperi
1615 Luxemburg
LUXEMBURG

Tel. (+352) 4398-1

Kontaktformular: eca.europa.eu/de/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors