Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zur „Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Sichere 5G-Einführung in der EU — Umsetzung des EU-Instrumentariums“

(COM(2020) 50 final)

(2020/C 429/37)

Berichterstatter: **Alberto MAZZOLA**

Mitberichterstatter: **Dumitru FORNEA**

Befassung	Europäische Kommission, 9.3.2020
Rechtsgrundlage	Artikel 304 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	3.9.2020
Verabschiedung im Plenum	16.9.2020
Plenartagung Nr.	554
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	217/0/2

1. **Schlussfolgerungen und Empfehlungen**

1.1. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) begrüßt die Initiative der Mitgliedstaaten und der Europäischen Kommission, den Stand der Umsetzung der in den Schlussfolgerungen zum EU-Instrumentarium empfohlenen strategischen und technischen Schlüsselmaßnahmen im Bereich der Sicherheit beim Ausbau des 5G-Ökosystems in den Mitgliedstaaten zu überprüfen.

1.2. Angesichts der zunehmenden Komplexität und Vielfalt der 5G-Anwendungen (die Kommission hat für 2025 folgende Konnektivitätsziele festgelegt: Schulen, Universitäten, Forschungszentren, Krankenhäuser, Hauptanbieter öffentlicher Dienste und stark von der Digitalisierung geprägte Unternehmen sollten über einen Internetzugang mit einer Down- und Uploadgeschwindigkeit von 1 Gigabit pro Sekunde verfügen; die privaten Haushalte im städtischen und ländlichen Raum sollten über einen Internetzugang mit einer Downloadgeschwindigkeit von mindestens 100 Megabit pro Sekunde verfügen; städtische Gebiete, Hauptverkehrsstraßen und Eisenbahnen sollten über eine ununterbrochene 5G-Abdeckung verfügen) ist der EWSA der Auffassung, dass sich eine solche Überprüfung des 5G-Ökosystems und der im Zuständigkeitsbereich der Kommission liegenden Maßnahmen zur Gewährleistung der Cybersicherheit von 5G-Netzen, einer diversifizierten 5G-Wertschöpfungskette, der technischen Normung und Zertifizierung, ausländischer Direktinvestitionen, des Schutzes von Handel und Wettbewerb, gemeinwirtschaftlicher Verpflichtungen, der öffentlichen Auftragsvergabe und der digitalen Diplomatie auf die geopolitische Sicherheit, die Sicherheit der Infrastrukturen und Daten und den Gesundheitsschutz, auch im Sinne von Artikel 168 Absatz 1 AEUV, erstrecken muss.

1.3. Nach Ansicht des EWSA ist es wichtig, dass das europäische 5G-Ökosystem Folgendes gewährleistet: Integrität, Vertraulichkeit, Zuständigkeiten für Leitung und Betrieb, Sicherheit, Fungibilität der Versorgung, Interoperabilität der Hardware- und Softwarekomponenten, gemeinsame technische und regulatorische Normen, Versorgungskontinuität, Zuverlässigkeit des Datenflusses und Datenschutz, Abdeckung in allen (auch dünn besiedelten) Gebieten, klare Kommunikation gegenüber Nutzern als aktiven Akteuren auf dem digitalen Markt, zügige Übernahme der Leitlinien der Internationalen Kommission zum Schutz vor nicht-ionisierender Strahlung (ICNIRP) im Sinne des Gesundheitsschutzes durch weitestgehende Verminderung von Strahlung. Die ICNIRP hat in den Leitlinien von 1998 den Teil über die Funkfrequenz und Exposition gegenüber elektromagnetischen Feldern (EMF) aktualisiert. In diesem Dokument werden diese überarbeiteten Leitlinien zum Schutz des Menschen vor Beeinträchtigungen durch EMF-Exposition im Bereich von 100 kHz bis 300 GHz dargestellt. Health Physics 118(5): 483-524; 2020- März 2020. Die ICNIRP (2020) hat eine Reihe von Änderungen vorgenommen, um zu gewährleisten, dass neue Technologien wie 5G unabhängig von unseren derzeitigen Annahmen keinen Schaden verursachen können.

1.4. Der EWSA ruft die Kommission auf, die Fortschritte beim Ausbau und bei der Nutzung von 5G genau zu überwachen. Er appelliert an die Mitgliedstaaten, den Prozess weiter zu beschleunigen, für eine verantwortungsvolle Umsetzung Sorge zu tragen und dabei alle sicherheits- und schutzrelevanten Aspekte zu berücksichtigen, so u. a. die Auswirkungen der 5G-Technologie auf die öffentliche Gesundheit und die lebenden Ökosysteme, die sozioökonomischen Folgen und die Auswirkungen auf den Wettbewerb, die Auswirkungen im Bereich der allgemeinen und beruflichen Bildung und die Wahrung der Grundrechte.

1.5. Der EWSA spricht sich dafür aus, dass die EU bei 5G, der nächsten Generation der Mobilfunktechnologie, zu einem weltweiten Vorreiter wird, der über eine sichere digitale Infrastruktur verfügt. Diese soll das wesentliche Fundament einer neuen, modernen europäischen Industriestrategie bilden, die sich durch einen radikalen Wandel bei der Mobilfunkanbindung auszeichnet. Außerdem besitzt sie ein enormes dynamisches Potenzial zur Stärkung der Produktivität und zur Förderung des Wachstums von Wirtschaft und Dienstleistungen im Interesse der Bürger.

1.6. Insbesondere ist es nach Ansicht des EWSA unerlässlich, die Risikoprofile der Anbieter zu bewerten und in der Folge Anbieter, die mit einem hohen Risiko behaftet sind, einschlägigen Beschränkungen zu unterwerfen, darunter den Ausschluss von Anbietern zur wirksamen Risikominderung und Haftungsfestlegung bei wichtigen Anlagen und Einrichtungen, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft werden.

1.7. Mittelfristig muss Europa in diesem Bereich zu einem autonomen Selbstversorger werden und zu diesem Zweck die Forschung und die Vielfalt europäischer Unternehmen umfassend fördern. Nach Ansicht des EWSA ist es wichtig, die EU-Mittel für die digitale FuI zu erhöhen und Investitionen der Betreiber und Anbieter in neue technische Sicherheitsfunktionen zu unterstützen. Damit einhergehend müssen Initiativen zur Stärkung der Sicherheit und Widerstandsfähigkeit der Systeme auf dem Markt anerkannt und vergütet werden.

1.8. Es ist wichtig, die Sicherheit für alle Mitgliedstaaten auch durch den Erhalt von Forschungszentren in mehreren Gebieten der EU zu gewährleisten. Der EWSA hält ferner an seiner Empfehlung fest, dass jedes Land mindestens zwei Anbieter haben sollte, davon mindestens ein europäisches Unternehmen, das die politische Sicherheit der Daten und die Erfüllung gesundheitspolitischer Erfordernisse gewährleisten kann.

1.9. Nach Auffassung des EWSA muss neben der Bedeutung, die zurecht den richtigen Maßnahmen im Hinblick auf die Befugnisse der nationalen Regulierungsbehörden und die Rolle der Telekommunikationsbetreiber eingeräumt wird, den Instrumenten für Nutzer, Bürger und einschlägige Organisationen der Zivilgesellschaft mehr Beachtung geschenkt werden, die spärlich und ineffizient sind. Ziel ist es, die Teilhabe und die Kompetenzen der Verbraucher zu stärken und sie zu proaktiven Akteuren auf dem Markt zu machen.

1.10. Die Kommission, das Europäische Parlament, der Rat und die Regierungen und Parlamente der Mitgliedstaaten müssen einen demokratischen Konsultationsrahmen schaffen, in dem der Öffentlichkeit die wissenschaftlichen und technischen Argumente und die rechtlichen Garantien erläutert und die Antworten der zuständigen Stellen auf die Fragen der Zivilgesellschaft gegeben werden können.

1.11. Der EWSA empfiehlt, die europäische digitale Diplomatie zu stärken, damit die EU ausgewogenere und auf Gegenseitigkeit beruhende Bedingungen für Handel und Investitionen gewährleisten kann, insbesondere in Bezug auf den Zugang von Unternehmen zum Markt, Beihilfen, die öffentliche Auftragsvergabe, Technologietransfers, gewerbliches Eigentum und sozial- und umweltrechtliche Vorschriften.

2. **Einleitung**

2.1. Die Sicherheit von 5G-Netzen ist für Bürger und Unternehmen, für den gesamten Binnenmarkt und für die technologische Souveränität der EU von strategischer Bedeutung. Bereits 2013 hat die Kommission die EU-Leitinitiative zur Einrichtung einer öffentlich-privaten 5G-Partnerschaft (ÖPP 5G) ins Leben gerufen, um die Forschung und Innovation im Bereich der 5G-Technologie zu beschleunigen.

2.2. Angesichts der weltweit mit 5G erwirtschafteten Umsätze, die 2025 einen Gegenwert von 100 Mrd. EUR übersteigen dürften, ist die 5G-Technik ein Schlüsselfaktor für die europäische Wettbewerbsfähigkeit auf dem Weltmarkt. Die Cybersicherheit der 5G-Netze ist daher für die strategische Autonomie der EU von entscheidender Bedeutung.

2.3. Die 5G-Netze bauen auf der derzeitigen Netztechnik der vierten Generation (4G) und der Glasfaser-Infrastruktur auf und bieten neue Dienstleistungskapazitäten. Sie werden zur zentralen Infrastruktur und Triebkraft für weite Teile der Wirtschaft der Union. Sie werden das Rückgrat eines breiten Spektrums von Diensten bilden, die für das Funktionieren des Binnenmarktes, die Aufrechterhaltung und Ausführung wichtiger wirtschaftlicher und gesellschaftlicher Funktionen (Energie, Verkehr, Bank- und Gesundheitswesen, Landwirtschaft, Fertigung, Vertrieb und Konsum) unverzichtbar sind.

2.4. Aufgrund der Schlüsselrolle der 5G-Netze beim digitalen Wandel der europäischen Wirtschaft und Gesellschaft, der Vernetzung und des transnationalen Charakters der Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen, sowie des grenzübergreifenden Charakters der betreffenden Bedrohungen würden sich alle erheblichen Schwachstellen und/oder Cybersicherheitsvorfälle, die 5G-Netze in einem Mitgliedstaat betreffen, auf die Union als Ganzes auswirken. Aus diesem Grund sollten Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus der 5G-Netze getroffen werden.

2.5. 2016 hat die Europäische Kommission mit einer Reihe von Initiativen (Mitteilung zur Gigabyte-Konnektivität für einen wettbewerbsfähigen digitalen Binnenmarkt — Hin zu einer europäischen Gigabit-Gesellschaft [1] [2] und Reform des Rechtsrahmens für die elektronische Kommunikation [3] und der Funktionen des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) [4], der Schwerpunkte der IKT-Normung für den digitalen Binnenmarkt [5] sowie Maßnahmen zur Förderung der Internetanbindung in Kommunen [6]) einen 5G-Aktionsplan der EU [7] verabschiedet, den der EWSA bereits begrüßt hat [8]. Ziel war es, die Bemühungen der EU beim Aufbau von 5G-Infrastrutkuren und -Diensten im digitalen Binnenmarkt mit einem Fahrplan für öffentliche und private Investitionen in die 5G-Infrastrukturen in der EU sowie mit dem Ziel zu untermauern, bis 2020 5G-Netze für kommerzielle Zwecke zu schaffen.

2.6. Gemäß der Definition in der Empfehlung [9] der Europäischen Kommission bezeichnet der Begriff 5G-Netze „eine Gesamtheit einschlägiger Netzinfrastrukturelemente, die auf weltweit vereinbarten technischen Normen für die Mobilfunk- und Drahtloskommunikation beruhen, für Netzanbindungs- und Mehrwertdienste verwendet werden und fortgeschrittene Leistungsmerkmale wie sehr hohe Datengeschwindigkeit und -kapazität, Kommunikation mit niedriger Latenzzeit, ultrahohe Zuverlässigkeit oder Unterstützung einer großen Zahl verbundener Geräte aufweisen“.

2.7. In der Empfehlung heißt es weiter, dass die Kommission die Umsetzung eines EU-Konzepts für die 5G-Cybersicherheit unterstützen und entsprechend der Forderung der Mitgliedstaaten alle ihr zur Verfügung stehenden Instrumente nutzen wird, um die Sicherheit der 5G-Infrastruktur und -Lieferkette zu gewährleisten:

— Telekommunikations-, Multimedia- und Cybersicherheitsvorschriften;

— Koordinierung im Bereich Normung und EU-weite Zertifizierung;

— Rahmen für die Überprüfung ausländischer Direktinvestitionen zum Schutz der europäischen 5G-Lieferkette;

— handelspolitische Schutzmaßnahmen;

— Wettbewerbsregeln;

— öffentliche Aufträge unter der Maßgabe, dass Sicherheitsaspekte gebührend berücksichtigt werden;

— EU-Förderprogramme unter der Maßgabe, dass Begünstigte die geltenden Sicherheitsanforderungen erfüllen.

2.8. Im Juli 2019 haben die Mitgliedstaaten die Ergebnisse ihrer nationalen Risikobewertungen der in der NIS-Richtlinie [10] vorgesehenen Kooperationsgruppe (aus Vertretern aller Mitgliedstaaten), der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) übermittelt. Diese enthielten Informationen über die wichtigsten Tätigkeiten, Bedrohungen und Schwachstellen im Einklang mit der Norm ISO/IEC 27005 in Bezug auf die 5G-Infrastruktur sowie die wichtigsten Risikoszenarien. Außerdem wurde beschrieben, inwiefern die Akteure, von denen die Bedrohungen ausgehen, bestimmte Schwachstellen einer Tätigkeit ausnutzen können. Diese nationalen Bewertungen wurden einer anschließenden koordinierten Bewertung und einem gemeinsamen Instrumentarium möglicher Risikominderungsmaßnahmen zugrunde gelegt.

2.9. Im Oktober 2019 hat die NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA in einem Bericht über die EU-weit koordinierte Risikobewertung zur Cybersicherheit in 5G-Netzen verschiedene wichtige sicherheitsrelevante Probleme ermittelt, die mit den wichtigsten technischen Innovationen in den Bereichen Software, Anwendungen und Dienstleistungen, mit der Rolle der Anbieter bei der Einführung und Nutzung von 5G-Netzen und mit dem Grad der Abhängigkeit von den einzelnen Anbietern zusammenhängen:

— zunehmende Verwundbarkeit durch Angriffe und mehr potenzielle Angriffspunkte;

— erhöhte Sensibilität aufgrund der neuen Struktur- und Funktionsmerkmalen von 5G-Netzen;

— Risiken im Zusammenhang mit der Abhängigkeit mobiler Netzbetreiber von den Anbietern und mit einer Zunahme der Angriffswege, die sich die Angreifer zunutze machen können;

---

[1] Artikel 168 Absatz 1 AEUV: „Die Tätigkeit der Union ergänzt die Politik der Mitgliedstaaten […]“.
[2] COM(2016) 587 final.
[3] COM(2016) 590 final.
[4] COM(2016) 591 final.
[5] COM(2016) 176 final.
[6] COM(2016) 589 final.
[7] COM(2016) 588 final.
[8] ABl. C 125 vom 21.4.2017, S. 74.
[9] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019, *Cybersicherheit der 5G-Netze* (ABl. L 88 vom 29.3.2019, S. 42).
[10] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

— Relevanz des Risikoprofils der einzelnen Betreiber im Hinblick auf eine mögliche Einflussnahme durch Drittstaaten;

— erhöhtes Risiko aufgrund der starken Abhängigkeit von den Anbietern im Hinblick auf eventuelle Versorgungsunterbrechungen, die durch handelspolitische Spannungen oder anderes verursacht werden;

— Bedrohungen im Zusammenhang mit der Verfügbarkeit und Integrität in den Bereichen Sicherheit, Vertraulichkeit und Datenschutz.

2.10. All diese Herausforderungen schaffen ein neues Sicherheitsparadigma, das eine Überprüfung des derzeitigen für den Sektor und sein Ökosystem geltenden Politik- und Sicherheitsrahmens erfordert und dazu führt, dass die Mitgliedstaaten die notwendigen Risikominderungsmaßnahmen ergreifen müssen.

2.11. Am 21. November 2019 veröffentlichte die ENISA den Bericht „Threat landscape for 5G networks" (Bedrohungslage der 5G-Netze), in dem sie die Bedrohungen im Zusammenhang mit der fünften Generation von Mobilfunknetzen bewertet und den Bericht der EU-Mitgliedstaaten ergänzt.

2.12. Am 29. Januar 2020 hat die NIS-Kooperationsgruppe das Instrumentarium „Cybersecurity of 5G networks — EU toolbox of risk mitigating measures" (EU-Instrumentarium für Maßnahmen zur Risikominderung) ([11]) mit einem möglichen gemeinsamen Maßnahmenpaket veröffentlicht, um die wichtigsten Cybersicherheitsrisiken von 5G-Netzen zu mindern und Leitlinien für die Auswahl von Maßnahmen zu geben, die in den Risikominderungsplänen auf nationaler und europäischer Ebene vorranging sein sollen. Am selben Tag nahm die Kommission eine Mitteilung zur Unterstützung des Instrumentariums ([12]) an, die Gegenstand dieser Stellungnahme ist.

2.13. Zu den wichtigsten Interessenträgern der 5G-Netzinfrastruktur gehören:

— Bürger, Verbraucher und Endnutzer von 5G;

— Mobilfunknetzbetreiber: Einrichtungen, die Mobilfunkdienste für Nutzer erbringen und das eigene Netz mit Unterstützung Dritter verwalten;

— Dienstleister für Mobilfunkbetreiber: Einrichtungen, die den Mobilfunkbetreibern Dienste bzw. Infrastrukturen anbieten, damit diese ihre eigenen Netze aufbauen und/oder verwalten können. Zu dieser Kategorie gehören die Hersteller von Telekommunikationsausrüstung, sonstige Drittanbieter wie Anbieter von Cloud-Infrastrukturen, Systemintegratoren, Auftragnehmer in den Bereichen Sicherheit und Instandhaltung und Hersteller von Übertragungsgeräten;

— Hersteller von vernetzten Geräten und die entsprechenden Dienstleister: Anbieter von Geräten bzw. Diensten, die das 5G-Netz nutzen (z. B. Smartphones, vernetzte Fahrzeuge, elektronische Gesundheitsdienste) und die entsprechenden Dienstkomponenten, die Gegenstand des 5G-Kontrollplans entsprechend der Netzwerkarchitektur „Mobile Edge Computing" sind;

— sonstige Interessenträger, einschließlich Dienste- und Inhalteanbietern.

Sie alle sind wichtige Interessenträger im Bereich Sicherheit, sowohl in Bezug auf den Beitrag zur Cybersicherheit von 5G-Netzen als auch als auch als potenzielle Angriffspunkte oder -vektoren. Deshalb ist es wichtig, die Risiken im Zusammenhang mit ihrer Stellung im 5G-Ökosystem zu bewerten.

2.14. Die wichtigsten konventionellen Bedrohungskategorien hängen mit dem Kompromiss zwischen Vertraulichkeit, Integrität und Verfügbarkeit zusammen. Genauer gesagt wurde festgestellt, dass eine Reihe von Bedrohungsszenarien im Zusammenhang mit 5G-Netzen insbesondere Folgendes betrifft:

— Störung des lokalen oder globalen 5G-Netzes (Verfügbarkeit);

— Datenspionage in der 5G-Netzinfrastruktur (Vertraulichkeit);

— Änderung oder Umleitung des Datenverkehrs in der 5G-Netzinfrastruktur (Integrität und/oder Vertraulichkeit);

— Zerstörung oder Veränderung anderer digitaler Infrastrukturen oder Informationssysteme durch 5G-Netze (Integrität und/oder Verfügbarkeit).

2.15. Bedrohungen, die von Staaten bzw. von staatlich unterstützten Akteuren ausgehen, wird die größte Beachtung geschenkt. Von diesen Akteuren gehen die schwersten und wahrscheinlichsten Bedrohungen aus, da sie u. U. Gründe, Absichten und vor allem die Fähigkeiten haben, nachhaltige und komplexe Angriffe auf die Sicherheit von 5G-Netzen zu verüben.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures

([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission

Auch wenn viele dieser Schwachstellen nicht 5G-spezifisch sind, ist es wahrscheinlich, dass ihre Anzahl und Bedeutung mit der Einführung von 5G-Netzen aufgrund der zunehmenden technischen Komplexität und der verstärkten Nutzung dieser Infrastruktur durch Wirtschaft und Gesellschaft zunehmen werden.

2.16. Da 5G-Netze weitgehend softwarebasiert sein werden, könnten die größten Sicherheitsmängel (z. B. mangelhafte Software-Entwicklungsprozesse bei den Geräteherstellern) dazu führen, dass die Angreifer leichter Backdoors in die Produkte einbauen und deren Erkennung erschweren können. Dadurch würde es wahrscheinlicher, dass deren Nutzung besonders schwerwiegende und weit verbreitete negative Auswirkungen hat. Vor dem Hintergrund, dass die Cybersicherheitsprobleme im Zusammenhang mit 4G noch nicht vollständig gelöst sind, könnten die Probleme mit 5G exponentiell zunehmen.

2.17. Darüber hinaus sind folgende Schwachstellen im Zusammenhang mit dem Prozess bzw. der Konfiguration zu berücksichtigen:

— Mangel an spezialisiertem und geschultem Personal für den Schutz, die Überwachung und die Instandhaltung der 5G-Netze;

— Mängel in Bezug auf angemessene interne Sicherheitskontrollen, Überwachungsmaßnahmen, Sicherheitsmanagementsysteme und Risikomanagement;

— unzureichende Sicherheits- oder Wartungsverfahren, wie Softwareupdates/Patch-Management in 5G-Netzen;

— Nichteinhaltung der 3GPP-Normen oder falsche Umsetzung von Normen;

— Netzkonstruktions- bzw. -strukturfehler, einschließlich fehlender wirksamer Notfall- und Kontinuitätsmechanismen, unzureichende oder fehlerhafte Konfiguration beispielsweise bei der Virtualisierung oder bei den Verwaltung- bzw. Zugangsrechten;

— ungeeignete Kriterien für den lokalen bzw. den Fernzugang zu Netzkomponenten;

— unzureichende Sicherheitsanforderungen bei der Beschaffung: dabei kann es sich um unangemessene Strategien für die Auswahl der Anbieter oder fehlende Priorisierung der Sicherheit gegenüber anderen Aspekten handeln.

2.18. Die Risikoprofile der einzelnen Anbieter müssen auf der Grundlage unterschiedlicher Faktoren bewertet werden: Möglichkeit der Einflussnahme auf Anbieter durch Drittstaaten, vor allem bei Anbietern mit enger Verbindung zur Regierung eines bestimmten Drittstaates; Rechtsvorschriften im Drittstaat, insbesondere dort, wo keine legislativen oder demokratischen Kontrollen und Gewaltenteilung bestehen und wo infolgedessen in der EU tätige Tochtergesellschaften eines Unternehmens wenig Neigung zur Befolgung der EU-Rechtsvorschriften haben könnten bzw. wo es keine Vereinbarungen zur Sicherheit oder zum Datenschutz zwischen der EU und dem betreffenden Drittstaat gibt; Aspekte der Eigentümerstruktur des Anbieters; Möglichkeiten des Drittstaats, in verschiedener Form Druck auszuüben, auch in Bezug auf den Herstellungsort der Ausrüstung; allgemeine Qualität der Produkte und Cybersicherheitsverfahren des Anbieters, einschließlich der Kontrolle der eigenen Zulieferkette und angemessene Priorisierung von Sicherheitsmaßnahmen.

2.19. Die Mitgliedstaaten haben die Umsetzung von Gegenmaßnahmen vereinbart, um auf die bereits ermittelten und möglichen künftigen Risiken angemessen und verhältnismäßig reagieren zu können. Insbesondere haben sie vereinbart, auf der Grundlage eines risikobasierten Ansatzes bestimmte Anforderungen oder Bedingungen für die Bereitstellung, den Ausbau und den Betrieb von 5G-Netzausrüstungen zu beschränken, zu verbieten und/oder vorzuschreiben.

2.20. Vor diesem Hintergrund sollten die Mitgliedstaaten

— die Sicherheitsanforderungen für Mobilfunknetzbetreiber verschärfen, (so u. a. strenge Zugangskontrollen, Vorschriften für sicheren Betrieb und sichere Überwachung, Beschränkungen für die Auslagerung bestimmter Funktionen usw.);

— die Risikoprofile der Anbieter nach objektiven, klaren Kriterien bewerten und in der Folge auf Anbieter, die als mit einem hohen Risiko behaftet gelten, einschlägige Beschränkungen im Einklang mit den Grundsätzen der Verhältnismäßigkeit und Rechtssicherheit anwenden, darunter den Ausschluss von Anbietern zur wirksamen Risikominderung bei wichtigen Anlagen und Einrichtungen, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft wurden;

— weltweit anerkannte und implementierte und einvernehmliche Sicherheitsstandards und bewährte Verfahren anwenden;

— sicherstellen, dass jeder Betreiber über eine angemessene herstellerneutrale Strategie verfügt, um eine größere Abhängigkeit von einem einzigen Anbieter (oder Anbietern mit ähnlichem Risikoprofil) zu vermeiden oder zu begrenzen;

— strenge Zugangskontrolle und sichere(n) Verwaltung, Betrieb und Überwachung des Netzes gewährleisten sowie die Zertifizierung von 5G-Komponenten und/oder -Prozessen nutzen; Diese Strategie muss auf einer von den Mitgliedstaaten und den Betreibern durchgeführten Risikoanalyse beruhen, damit die Wahl einer herstellerneutralen Strategie nicht das Risikoniveau in dem Betreibernetz erhöht;

— für ein angemessenes Gleichgewicht zwischen den Anbietern auf nationaler Ebene sorgen und die Abhängigkeit von mit einem hohen Risiko behafteten Anbietern vermeiden — u. a. durch die Förderung einer größeren Interoperabilität der Ausrüstungen;

— eine diversifizierte und solide 5G-Lieferkette unterhalten, um eine langfristige Abhängigkeit zu vermeiden, und zwar durch die umfassende Nutzung der EU-Instrumente zur Überprüfung ausländischer Direktinvestitionen, handelspolitischer Schutzinstrumente, Wettbewerbsregeln und EU-Vorschriften über öffentliche Aufträge;

— die internen Kapazitäten der EU im Bereich der 5G-Technik und deren Folgetechnik durch Nutzung der einschlägigen EU-Programme und -Fördermittel weiter stärken; die Koordinierung zwischen den Mitgliedstaaten im Bereich der Normung durch die Stärkung der Test- und Auditkapazitäten erleichtern, um spezifische Sicherheitsziele zu erreichen und einschlägige EU-weite Zertifizierungssysteme zu entwickeln — im Einklang mit den Vorschriften zur Cybersicherheit und im Sinne der Förderung der Interoperabilität.

2.21. Wie die Kommission mehrfach betont hat, ist und bleibt der europäische Binnenmarkt für alle, die nach Europa kommen wollen, offen, unter der Voraussetzung, dass sie klare und strikte Vorschriften einhalten, die auf objektiven Kriterien beruhen.

2.22. Am 6. Juni 2020 hat der Rat hervorgehoben, dass es wichtig ist, die Souveränität und Zusammenarbeit in der EU zu stärken und mithilfe von EU-Programmen wie der Fazilität „Connecting Europe“ und dem Programm „Digitales Europa“ Synergien zu schaffen und die digitalen Kompetenzen sowie die digitale Wirtschaft auszubauen. Zudem betonte er die Bedeutung der künstlichen Intelligenz und der Cybersicherheit sowie der aktiven Rolle der Digitalisierung für das Erreichen der Ziele des Grünen Deals.

3. **Die Mitteilung der Kommission**

3.1. Als Reaktion auf das 5G-Instrumentarium der NIS-Kooperationsgruppe

— wird die Kommission entsprechend der Forderung der Mitgliedstaaten alle ihr zur Verfügung stehenden Instrumente nutzen, um erforderlichenfalls die Sicherheit der 5G-Infrastruktur und -Lieferkette zu gewährleisten;

— fordert die Kommission die Mitgliedstaaten und die Institutionen auf, für die Umsetzung wirksamer Strategien zur Risikominderung zu sorgen und weitere Koordinierungsmaßnahmen auf EU-Ebene zu ergreifen, um einen konzertierten Ansatz für die 5G-Cybersicherheit zu gewährleisten;

— ruft die Kommission die Mitgliedstaaten auf, Schritte zur Umsetzung aller in den Schlussfolgerungen zum EU-Instrumentarium empfohlenen Maßnahmen zu unternehmen und einen gemeinsamen Bericht über deren Umsetzung vorzubereiten, während die NIS-Kooperationsgruppe die Umsetzung des EU-Instrumentariums weiterhin unterstützen wird;

— plant die Kommission im Rahmen ihrer Zuständigkeiten Maßnahmen zur Gewährleistung der Cybersicherheit von 5G-Netzen und einer diversifizierten 5G-Wertschöpfungskette, der technischen Normung und Zertifizierung, ausländischer Direktinvestitionen und handels- und wettbewerbspolitischen Schutzes, der Auftragsvergabe und Cyberdiplomatie sowie der eigenen Programme und einschlägigen Fonds insbesondere für die Bereiche FuI, Zusammenhalt und Entwicklung.

4. **Allgemeine Bemerkungen**

4.1. Der EWSA ist überzeugt, dass die neuen 5G-Technologien die Art, wie wir mit der Welt interagieren, verändern können. Sie bieten Möglichkeiten für neue Anwendungen, Geschäftsmodelle, Lebensstile, intelligente Fabriken, höhere Produktivität und Dienste von neuer Qualität für die Bürgerinnen und Bürger. Sie können den Weg für bahnbrechende Technologien wie automatisierte Fahrzeuge und fortschrittliche Herstellungs- und Vertriebssysteme ebnen und die Vernetzung Tausender von Geräten ermöglichen, die im Rahmen des Internets der Dinge Teil unseres Alltags werden dürften. Der EWSA würde jedoch begrüßen, dass die Kommission die Wirkungs- und Durchführbarkeitsstudien sowie Kosten-Nutzen-Analysen von 5G im Vergleich zur Nutzung der 4G-Technologie bzw. der Glasfaserkommunikation intensiviert. Der EWSA hält es für wesentlich, dass die 5G-Technik darauf ausgerichtet wird, eine bessere kreislauforientierte Ressourcennutzung zu erreichen und ihren großen energiebezogenen CO_2-Fußabdruck zu verringern. Aus Sicht des EWSA ist es wichtig, den Strukturwandel in der Gesellschaft zu bewältigen, indem ein fairer und reibungsloser Übergang gefördert und die Qualifikationslücke geschlossen wird, um besser bezahlte, flexible und hochqualifizierte Arbeitsplätze zu schaffen.

4.2. Die dreifachen Risiken — unkontrollierte Pandemien, unzureichende wirtschaftspolitische Rahmenbedingungen, geopolitische „schwarze Schwäne" — könnten zu einer anhaltenden Weltwirtschaftskrise und zu Zusammenbrüchen der Finanzmärkte bzw. Fluchtbewegungen aus diesen führen. Gleichzeitig werden sich alle Teile der europäischen Gesellschaft zunehmend bewusst, dass für eine nachhaltige Wirtschaftsentwicklung und für **die stattfindende digitale Revolution, bei der 5G-Netze eines der wichtigsten Instrumente darstellen**, Modalitäten nötig sind, die sowohl der technologischen Souveränität als auch der Produktivitätssteigerung und einer effizienteren Nutzung von Ressourcen gerecht werden, die — durch einen angemessenen Rechtsrahmen sowie einen entsprechenden wirtschaftlich-finanziellen Rahmen flankiert — zur Verfügung stehen können.

4.3. Der EWSA fordert die EU-Organe und die Mitgliedstaaten auf, den digitalen Binnenmarkt zu vollenden und dazu Kapazitäten zur Integration und Nutzung der 5G-Dienste zur Erhaltung und Stärkung der Wettbewerbsfähigkeit der europäischen Wirtschaft zu entwickeln. Er ruft die Kommission auf, die Fortschritte beim Ausbau und bei der Nutzung von 5G genau zu überwachen. Der Ausschuss appelliert an die Mitgliedstaaten, den Prozess weiter zu beschleunigen und dabei alle sicherheits- und schutzrelevanten Aspekte zu berücksichtigen, so u. a. die Auswirkungen der 5G-Technologien auf die öffentliche Gesundheit und die lebenden Ökosysteme, die sozioökonomischen Folgen und die Auswirkungen auf den Wettbewerb, die Auswirkungen im Bereich der allgemeinen und beruflichen Bildung und die Wahrung der Grundrechte (Recht auf Eigentum, Recht auf Privatsphäre, Schutz personenbezogener Daten u. a.).

4.4. Der EWSA spricht sich dafür aus, dass die EU bei 5G, der nächsten Generation der Mobilfunktechnologie, eine weltweite Führungsrolle einnimmt und über eine sichere digitale Infrastruktur verfügt. Diese soll als wesentliches Fundament für eine neue moderne europäische Industriestrategie dienen, die sich durch einen radikalen Wandel bei der Mobilfunkanbindung auszeichnet und mit einem enormen dynamischen Potenzial zur Stärkung der Produktivität und zur Förderung des Wachstums von Wirtschaft und Dienstleistungen im Interesse der Bürger, ihres Wohlergehens und des Klima- und Umweltschutzes einhergeht. Die EU muss dadurch eine Führungsrolle bei der 5G-Revolution einnehmen.

4.5. Da Cybersicherheit und nationale Sicherheit untrennbar miteinander verbunden sind, ist der EWSA der Auffassung, dass alle Entscheidungen über die nationale Sicherheit eines EU-Mitgliedstaates unter Berücksichtigung des EU-Kontextes getroffen werden müssen. Die nichttechnischen Bewertungen müssen objektiv auf der Grundlage von Risikobewertungskriterien angewandt werden, die auf europäischer Ebene festgelegt werden und erforderlich sind, um einen verlässlichen und harmonisierten Rechtsrahmen in ganz Europa sicherzustellen, der die volle Interoperabilität gewährleistet.

4.6. Nach Auffassung des EWSA haben die Informationsqualität und die Kommunikationsmodalitäten (der so genannte Framing-Effekt: Einrahmungseffekt bzw. Präferenzordnung, Salienz) einen beträchtlichen Einfluss auf die Verhaltensoptionen der Empfänger. Das Ziel, die Teilhabe der Verbraucher zu fördern, geht mit der Ermittlung von Informationsmaßnahmen und Instrumenten zur Stärkung ihrer Fähigkeiten einher, damit sie als aktive Player auf dem digitalen Markt auftreten können. Der EWSA weist auf die Notwendigkeit hin, den Bürgerinnen und Bürgern aktuelle und korrekte Informationen über die Vorteile und Risiken von 5G zu geben, die auf einem breiten wissenschaftlichen Konsens beruhen. Aspekte, in denen ein solcher Konsens ungewiss ist, sollten ebenfalls aufgezeigt werden.

4.7. Der EWSA ist überzeugt, dass der Zugang zum europäischen digitalen Markt auch in Zukunft allen Unternehmen diskriminierungsfrei offenstehen muss, wobei aber ein europäischer Rahmen von Regeln und Vorschriften sowie festen und klaren Bewertungs- und Sicherheitskriterien eingehalten werden muss, die die Wiedererlangung und Neubelebung von Europas technologischer Souveränität wieder in den Mittelpunkt der EU-Strategie stellen.

4.8. Zu den fünf wichtigsten Infrastrukturanbietern gehören zwar zwei europäische, zwei chinesische und ein koreanischer Anbieter ([13]), doch unter den Herstellern von 5G-Geräten und -Chipsätzen ist kein europäisches Großunternehmen zu finden. Der EWSA ist davon überzeugt, dass es unter der Vielzahl von Anbietern mindestens einen mit einem europäischen Mutterunternehmen geben muss und dass auch ein Rahmen für die Interoperabilität und vollständige Ersetzbarkeit von Hardware- und Softwarekomponenten geschaffen werden muss, um im Rahmen einer starken internationalen Zusammenarbeit und der uneingeschränkten Gegenseitigkeit von Offenheit, Zugang und Betrieb auf den Märkten die uneingeschränkte technologische Souveränität Europas zu gewährleisten. Eine solche Diversifizierung kann angewandt werden, solange die Interoperabilität der Dienste möglich ist und die Cybersicherheitsrisiken durch die Vielfalt nicht erhöht werden.

4.9. Mittelfristig muss Europa in diesem Bereich zu einem autonomen Selbstversorger werden und zu diesem Zweck die Forschung und die Vielfalt europäischer Unternehmen umfassend fördern. Der EWSA begrüßt das von den Mitgliedstaaten vereinbarte Maßnahmenpaket zur Bewältigung der Sicherheits- und Schutzrisiken im Zusammenhang mit der Einführung der 5G-Technologie, die bereits im Rahmen der europäischen Bewertung ermittelt wurden. Er ist allerdings der Auffassung, dass die strengen und sicheren Expositionsgrenzwerte für elektromagnetische Felder, die auf EU-Ebene empfohlen werden und auf aktualisierten Leitlinien der von der Weltgesundheitsorganisation (WHO) anerkannten ICNIRP beruhen, für alle Frequenzbänder für 5G gelten sollten ([14]): Die ICNIRP-Grenzwerte beruhen auf dem Vorsorgeprinzip, da sie 50 Mal niedriger sind als die auf der Grundlage der verfügbaren wissenschaftlichen Erkenntnisse ermittelten Werte für die Auswirkungen auf die öffentliche Gesundheit.

([13]) Die fünf weltweiten Anbieter sind derzeit Ericsson, Nokia, Huawei, ZTE und Samsung.

([14]) EP — E-003040/2019 Antwort von Frau Kyriakides im Namen der Europäischen Kommission (17.1.2020).

4.10. Der EWSA stellt jedoch fest, dass die ICNIRP-Leitlinien nicht von allen Interessenträgern anerkannt werden, zumal sich einige Wissenschaftler nach dem ALARA-Prinzip („as low as reasonably achievable", so niedrig wie nach vernünftigem Ermessen erreichbar) für wesentlich strengere Grenzwerte für die Exposition der Bevölkerung einsetzen. Die Lösung, die zur Ergänzung der 5G-Kommunikationsinfrastrukturen vorgeschlagen werden könnte, umfasst die Nutzung fester Datenverbindungen durch existierende Technologien ohne Funktechnik (Ethernet-Verkabelung, Glasfaser usw.) bei ortsfester Nutzung (z. B. Geldautomaten, Bankterminals, Industrieroboter, ferngesteuerte medizinische Roboter usw.) und in Situationen, in denen Nutzer von Big-Data-Übertragungen tätig sind (Anbieter digitaler Dienste, Unternehmen usw.) sowie das Internet der Dinge an festen, nichtmobilen Standorten (Smart Home, Smart City, Sensoren auf öffentlichen Versorgungseinrichtungen usw.).

4.11. Die Kommission, das Europäische Parlament, der Rat und die Regierungen und Parlamente der Mitgliedstaaten müssen einen demokratischen Konsultationsrahmen schaffen, in dem der Öffentlichkeit die wissenschaftlichen und technischen Argumente und die rechtlichen Garantien erläutert und die Antworten der zuständigen Stellen auf die Fragen der Zivilgesellschaft gegeben werden können.

4.12. Nach Auffassung des EWSA muss neben der Bedeutung, die zurecht den richtigen Maßnahmen im Hinblick auf die Befugnisse der nationalen Regulierungsbehörden und die Rolle der Telekommunikationsbetreiber eingeräumt wird, den Instrumenten für Nutzer, Bürger und einschlägige Organisationen der Zivilgesellschaft mehr Beachtung geschenkt werden, die spärlich und ineffizient sind.

4.13. Der EWSA hat das Problem der elektromagnetischen Hypersensitivität (EHS) anerkannt ([15]) und diesbezüglich seine Sorge zum Ausdruck gebracht. Er begrüßt, dass das Problem und seine Ursachen weiter eingehend erforscht werden, und hat die Kommission eindringlich dazu aufgerufen, die Arbeiten in diesem Bereich fortzusetzen und auszubauen.

4.14. Die Glaubwürdigkeit der Anbieter von 5G-Telekommunikations- und Anwendungsdiensten ist von wesentlicher Bedeutung, da das Online-Informationsmanagement die Grundlage für Dienste zur Aggregation von Daten bildet, die von den Nutzern erhoben und verarbeitet werden, und zwar mithilfe von technischen, rechtlichen und steuerlichen Mechanismen unter Verknüpfung von Gegenständen, Maschinen und Algorithmen.

4.15. Der EWSA hat vorgeschlagen ([16]), den Begriff „Eigentum an Daten" zu vermeiden und lieber eine Definition der „Rechte an Daten" von natürlichen und juristischen Personen festzulegen. Die Verbraucher sollten die Kontrolle über die von vernetzten Geräten generierten Daten haben, um den Schutz der eigenen Privatsphäre in Verbindung mit der Zugänglichkeit, Interoperabilität und Übertragung von Daten zu gewährleisten und ausreichenden Datenschutz und Schutz der Privatsphäre sowie einen fairen Wettbewerb und eine größere Auswahl für die Verbraucher sicherzustellen.

4.16. Die Datenschutz-Grundverordnung (DSGVO) sollte durch klare Umsetzungsleitlinien ergänzt werden, um eine einheitliche Anwendung und ein hohes Maß an Daten- und Verbraucherschutz im Hinblick auf die Interkonnektivität von Geräten und Gegenständen zu erreichen. Außerdem sollten die Vorschriften über die Haftpflicht und die Versicherung von Produkten überarbeitet und an die Tatsache angepasst werden, dass Entscheidungen zunehmend von Softwareanwendungen in einem gänzlich sicheren Umfeld getroffen werden.

4.17. Nach Auffassung des EWSA ist es ausschlaggebend, dass die Mitgliedstaaten die strategischen und technischen Empfehlungen des EU-Instrumentariums befolgen. Sie sollten von spezifischen nationalen Ansätzen wie zusätzlichen Tests und Zertifizierungen absehen, da dies zu einer Fragmentierung des Marktes und Verzögerungen bei der Umsetzung der Technologien sowie Inkohärenzen zwischen den Märkten führen würde und das Vertrauen in die Prüf- und Zertifizierungssysteme untergraben könnte.

4.18. Nach Auffassung des EWSA sollte auf globale Standards — mit verstärkter europäischer Unterstützung — und gemeinsame und anerkannte bewährte Verfahren zurückgegriffen werden, um Bedrohungen wirksam begegnen zu können, Skaleneffekte zu erzielen, eine Fragmentierung zu vermeiden und die Interoperabilität der europäischen Systeme sicherzustellen. Die Beratungen über die technischen Standards dienen einer notwendigen Präzisierung, die es den Unternehmen ermöglichen wird, wieder wettbewerbsfähig zu werden und diese wichtige Arbeit zu leisten, die die Einführung fortgeschrittener Technologien wie 5G und künstliche Intelligenz (KI) auf allen Märkten ermöglicht.

4.19. Insbesondere ist es nach Ansicht des EWSA unerlässlich, die Risikoprofile der Anbieter zu bewerten und in der Folge Anbieter, die mit einem hohen Risiko behaftet sind, einschlägigen Beschränkungen zu unterwerfen, darunter den Ausschluss von Anbietern zur wirksamen Risikominderung bei wichtigen Anlagen und Einrichtungen, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft werden.

4.20. Nach Ansicht des EWSA ist es wichtig, die Investitionen der Betreiber und Anbieter in neue technische Sicherheitsfunktionen zu erhöhen. Damit einhergehend müssen Initiativen zur Stärkung der Sicherheit und Widerstandsfähigkeit der Systeme auf dem Markt anerkannt und vergütet werden. Eine stärkere Sichtbarkeit von Investitionen in die Sicherheit könnte neue Marktvorteile bringen.

([15]) ABl. C 242 vom 2.7.2015, S. 31.
([16]) ABl. C 353 vom 18.10.2019, S. 79.

4.21. Der Ausschuss unterstützt nachdrücklich gemeinsame Maßnahmen zur Unterstützung der industriellen Entwicklung und der Einführung von 5G: Bewertung von Marktversagen oder Marktlücken entlang der 5G-Wertschöpfungskette, die gezielte Maßnahmen im Rahmen des nächsten langfristigen Haushalts oder ein mögliches Projekt von gemeinsamem europäischem Interesse zur 5G-Cybersicherheit rechtfertigen würden (Schutz und Sicherheit).

4.22. Der EWSA betont, dass sich die digitale Infrastruktur während der COVID-19-Krise zwar als widerstandsfähig und robust erwiesen hat, dass jedoch weitere Investitionen in die 5G-Infrastruktur erforderlich sind, um die nach wie vor bestehende digitale Kluft zu überwinden, die den Zugang der Bürger zu elektronischen Gesundheitsdiensten, eLearning und Telearbeit einschränken kann.

4.23. In Bezug auf die technologische Diplomatie hält es der Ausschuss für wesentlich, dass die EU für ausgewogenere und auf Gegenseitigkeit beruhende Bedingungen für Handel und Investitionen sorgt, insbesondere in Bezug auf Marktzugang von Unternehmen, Subventionen, öffentliches Beschaffungswesen, Technologietransfer, gewerbliches Eigentum sowie Sozial- und Umweltnormen, insbesondere im Hinblick auf „Systemrivalen, die alternative Governance-Modelle fördern", wobei ein ungehinderter Wettbewerb und die technische Innovation im Markt zu fördern sind.

4.24. Der EWSA unterstützt nachdrücklich die Notwendigkeit, eine diversifizierte und solide 5G-Lieferkette mit mehreren austauschbaren und interoperablen Anbietern zu unterhalten, um eine langfristige Abhängigkeit zu vermeiden, und im Finanzrahmen 2021-2027 die Programme und Initiativen zum Kapazitätsaufbau und die europäische technologische Souveränität im Bereich der 5G-Technik und deren Folgetechnik weiter zu stärken.

4.25. Im Rahmen des am 27. Mai 2020 angenommenen Aufbauprogramms für Europa wird der Index 2020 für die digitale Wirtschaft und Gesellschaft (DESI) als Grundlage für die länderspezifische Analyse zur Unterstützung der digitalen Empfehlungen des Europäischen Semesters dienen. Dies wird den Mitgliedstaaten helfen, ihren Reform- und Investitionsbedarf gezielt auszurichten und zu priorisieren, wodurch der Zugang zu der mit 560 Mrd. EUR ausgestatteten Aufbau- und Resilienzfazilität erleichtert wird. Mit dieser Fazilität werden den Mitgliedstaaten Mittel zur Verfügung gestellt, um ihre Volkswirtschaften widerstandsfähiger zu machen und sicherzustellen, dass Investitionen und Reformen den ökologischen und digitalen Wandel unterstützen. Da die Pandemie erhebliche Auswirkungen auf alle fünf DESI-Dimensionen hatte, sollten die Schlussfolgerungen von 2020 für 5G in Verbindung mit den zahlreichen Maßnahmen gesehen werden, die die Kommission und die Mitgliedstaaten zur Bewältigung der Krise und zur Unterstützung der Erholung ergriffen haben.

Brüssel, den 16. September 2020

Der Präsident
des Europäischen Wirtschafts- und Sozialausschusses
Luca JAHIER