Rat der
Europäischen Union

Brüssel, den 30. Januar 2020
(OR. en)

5664/20

TELECOM 9
CYBER 12
COMPET 20
MI 16
CONSOM 13

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	30. Januar 2020
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2020) 50 final
Betr.:	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

Die Delegationen erhalten in der Anlage das Dokument COM(2020) 50 final.

Anl.: COM(2020) 50 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 29.1.2020
COM(2020) 50 final

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

1. Einleitung

Die fünfte Generation (5G) der Telekommunikationsnetze wird eine wesentliche Rolle bei der Entwicklung der europäischen Gesellschaft und Wirtschaft spielen. 5G-Netze werden voraussichtlich enorme wirtschaftliche Chancen bieten und eine wichtige Grundlage für den digitalen und ökologischen Wandel in Bereichen wie Verkehr, Energie, Fertigung, Gesundheit, Landwirtschaft und Medien bilden.

Die 5G-Technik wird sich daher potenziell auf alle Aspekte des Lebens der EU-Bürgerinnen und -Bürger auswirken. Die Cybersicherheit der 5G-Netze ist daher nicht nur für den Schutz unserer Volkswirtschaften, Gesellschaften und demokratischen Prozesse unverzichtbar, sondern bildet auch die Voraussetzung für einen vertrauensvollen digitalen Wandel zum Nutzen aller Bürgerinnen und Bürger der EU.

Aufgrund der Abhängigkeit vieler kritischer Dienste von 5G-Netzen wären die Folgen systemischer und weitverbreiteter Störungen besonders schwerwiegend und können angesichts der Vernetzung der digitalen Ökosysteme auch erhebliche Auswirkungen über nationale Grenzen hinaus haben. Die Gewährleistung der Cybersicherheit der 5G-Netze ist daher ein Thema von strategischer Bedeutung für die Union in einer Zeit, in der Cyberangriffe zunehmen, immer komplexer werden und von einem breiten Spektrum von Akteuren ausgehen, insbesondere Akteuren, die von Nicht-EU-Staaten geführt oder unterstützt werden. Für die Sicherheit kritischer Infrastrukturen wie 5G besteht der gewählte Ansatz darin, erstmals ein gemeinsames europäisches Vorgehen festzulegen. Bei diesem Vorgehen bleibt die Offenheit des EU-Binnenmarkts in vollem Umfang gewahrt, solange die risikobasierten Sicherheitsanforderungen der EU eingehalten werden.

Der Europäische Rat rief auf seiner Tagung am 22. März 2019 zu einem abgestimmten Vorgehen bei der Sicherheit von 5G-Netzen auf. Am 26. März 2019 nahm die Kommission ihre Empfehlung (EU) 2019/534 zur Cybersicherheit der 5G-Netze[1] an. Darin rief sie Mitgliedstaaten auf, ihre nationalen Risikobewertungen abzuschließen und ihre nationalen Maßnahmen zu überprüfen sowie auf EU-Ebene zusammenzuarbeiten, um eine koordinierte Risikobewertung und ein Instrumentarium möglicher Maßnahmen zur Risikominderung zu erarbeiten. Diese Mitteilung ist fester Bestandteil der umfassenden europäischen Digitalstrategie der Kommission, wie sie der Europäische Rat gefordert hat.

2. 5G-Einführung in der EU

Die Einführung von 5G-Netzinfrastrukturen in Europa ist für die europäische Industriestrategie und für die Wettbewerbsfähigkeit Europas von zentraler Bedeutung. Die Kommission sieht die Einführung von 5G-Netztechnik als wichtige Voraussetzung für künftige digitale Dienste. Im Jahr 2016 nahm die Kommission ihren 5G-Aktionsplan an, um dafür zu sorgen, dass die Union über die erforderlichen Vernetzungsinfrastrukturen für ihren digitalen Wandel (ab 2020) und für die flächendeckende 5G-Einführung in städtischen Gebieten und entlang der Hauptverkehrswege (ab 2025) verfügt[2]. In ihrer Mitteilung zur Gigabit-Gesellschaft formulierte die Kommission das ehrgeizige Ziel, eine flächendeckende

[1] Empfehlung (EU) 2019/534 der Kommission zur Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

[2] COM(2016) 588 vom 14.9.2016: Mitteilung der Kommission „5G für Europa: ein Aktionsplan".

Anbindung an Mobilfunk-Datendienste – auch in ländlichen und abgelegenen Gebieten – zu verwirklichen[3].

Was die Zuweisung von Funkfrequenzen betrifft, haben die Mitgliedstaaten bislang 16 % der 5G-Pionierbänder zugewiesen[4]. Angesichts der bestehenden rechtlichen Verpflichtung, die Nutzung aller 5G-Pionierbänder bis Ende des Jahres zu erlauben, sind in den nächsten Monaten Konsultationen für eine ganze Reihe von Zuweisungsverfahren zu erwarten.

Europa gehört bei der kommerziellen Einführung von 5G-Diensten zu den am weitesten fortgeschrittenen Regionen der Welt[5]. Derzeit wird davon ausgegangen, dass die ersten 5G-Dienste bis Ende 2020 in 138 europäischen Städten verfügbar sein werden. Die ersten 5G-Netze bauen noch auf der derzeitigen Netztechnik der 4. Generation (4G) auf. 5G-Dienste werden zunächst hauptsächlich für die breite Öffentlichkeit bereitgestellt, entweder als Verbesserung der Kapazität und Geschwindigkeit gegenüber 4G oder als kostengünstige drahtlose Alternative zu Festnetzen[6].

In Bezug auf neue Unternehmensdienstleistungen, z. B. in den Bereichen Energie, Lebensmittel und Landwirtschaft, Gesundheit, Fertigung oder Verkehr, ist Europa mit seinen Investitionen in einer Größenordnung von 1 Mrd. EUR gut vorangekommen. Dazu zählen auch EU-Mittel in Höhe von 300 Mio. EUR, die im Rahmen von Horizont 2020 für die öffentlich-private Partnerschaft für 5G zur Verfügung stehen. Zu diesen Investitionen gehören mehr als 160 groß angelegte 5G-Erprobungen in ganz Europa, darunter zehn grenzüberschreitende Autobahnkorridore für eine groß angelegte Erprobung 5G-gestützter, vernetzter und automatisierter Mobilitätsdienste. Erprobt werden 5G-gestützte Anwendungen in vielfältigen Bereichen: von nachhaltiger Gesundheitsversorgung und automatisierter Mobilität bis hin zur ressourceneffizienten Landwirtschaft, intelligenten Stromnetzen und der Industrie 4.0. Außerdem stellte die EIB mit Unterstützung des Europäischen Fonds für strategische Investitionen Darlehen zur Beschleunigung der Forschung und Entwicklung im Bereich der 5G-Technik bereit.

Der Europäische Kodex für die elektronische Kommunikation (im Folgenden der „Kodex“)[7], der ab dem 21. Dezember 2020 gelten wird, ist eine wichtige Grundlage für die Schaffung eines investitionsfreundlichen Umfelds nicht nur für 5G-Netze. Darüber hinaus werden öffentliche Förderprogramme wie der digitale Teil der Fazilität „Connecting Europe“[8] oder die Europäischen Struktur- und Investitionsfonds ebenfalls eine wichtige Rolle beim

---

3 COM(2016) 587: Mitteilung der Kommission „Konnektivität für einen wettbewerbsfähigen digitalen Binnenmarkt – Hin zu einer europäischen Gigabit-Gesellschaft“.

4 http://www.5GObservatory.eu

5 http://www.5GObservatory.eu

6 Einige der neuen Funktionen der 5G-Technik werden dann schrittweise eingeführt. In einer ersten Phase (sehr kurzfristig oder kurzfristig) wird die 5G-Einführung in erster Linie „nicht eigenständige“ Netze umfassen, bei denen nur das Funkzugangsnetz auf 5G-Technik aufgerüstet wird, die ansonsten aber noch auf bestehenden 4G-Kernnetzen beruhen und den Endnutzern eine bessere breitbandige Mobilfunkleistung bieten. In den folgenden Phasen (kurz-/mittel- bis langfristig) wird der Aufbau „eigenständiger“ 5G-Netze mit den 5G-Kernnetzfunktionen eine viel umfassendere Änderung der Netzarchitektur erforderlich machen und mit der Zeit bewirken.

7 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation (Neufassung).

8 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Schaffung der Fazilität „Connecting Europe“ und zur Aufhebung der Verordnungen (EU) Nr. 1316/2013 und (EU) 283/2014, COM(2018) 438 vom 6.6.2018.

künftigen Ausbau der 5G-Netze spielen, denn sie werden insbesondere die Anbindung von Nutzergemeinschaften wie Schulen, Krankenhäusern, Städten und lokalen Verwaltungen an 5G-gestützte Dienste voranbringen.

Angesichts der strategischen Möglichkeiten, die sich in Europa im Bereich der 5G-Dienste für verschiedene Wirtschaftszweige bieten, wird es entscheidend darauf ankommen, dass Netzbetreiber und Diensteanbieter in modernste Lösungen für 5G-Netze und 5G-Dienste investieren. Als Voraussetzung hierfür werden aber nicht nur neue 5G-Funknetze, sondern auch neue sogenannte „eigenständige" 5G-Kernnetze gebraucht, damit fortgeschrittene 5G-Funktionen wie Network-Slicing[9] und Edge-Computing[10] realisiert werden können.

Die Kommission wird die erfolgreiche 5G-Einführung in der EU weiterhin nachdrücklich unterstützen und dazu unter anderem auf die Mitgliedstaaten und Interessenträger zugehen, damit die Chancen der 5G-Technik ergriffen werden können. Dabei wird sie nach dem Vorsorgeprinzip[11] und in Zusammenarbeit mit den einschlägigen internationalen Organisationen und den Wissenschaftskreisen relevante Gesundheitsaspekte gebührend berücksichtigen.

3. Die EU-weit koordinierte Risikobewertung zur Cybersicherheit in 5G-Netzen

Im Rahmen der Zusammenarbeit in der NIS[12]-Kooperationsgruppe hat jeder Mitgliedstaat seine eigene nationale Risikobewertung seiner 5G-Netzinfrastrukturen abgeschlossen und die Ergebnisse Anfang Juli 2019 der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) übermittelt.

Auf der Grundlage dieser nationalen Risikobewertungen veröffentlichte die NIS-Kooperationsgruppe, die aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA besteht, am 9. Oktober 2019 einen Bericht über die EU-weit koordinierte Risikobewertung zur Cybersicherheit in 5G-Netzen[13]. Darin werden die Hauptbedrohungen und deren Verursacher, die anfälligsten Anlagen und Einrichtungen sowie die wichtigsten Schwachstellen (technischer und anderer Art) aufgezeigt, von denen 5G-Netze betroffen sind. Auf dieser Grundlage werden in dem Bericht auch Risikokategorien genannt, die aus EU-Sicht von strategischer Bedeutung sind. Diese werden anhand konkreter Risikoszenarien veranschaulicht, die für die verschiedenen Einrichtungen und Anlagen relevante Kombinationen der verschiedenen Parameter (Schwachstellen, Bedrohungen und deren Verursacher) darstellen (siehe Anlage).

---

9 5G-Network-Slicing ermöglicht eine hochgradige Trennung verschiedener Dienste-Schichten in demselben physischen Netz und steigert somit die Möglichkeiten, differenzierte Dienste über das gesamte Netz anzubieten.

10 Edge-Computing bezeichnet ein Konzept der dezentralen Datenverarbeitung, bei dem Rechenleistung und Datenspeicher näher an den Ort verlagert werden, an dem sie benötigt werden, um die Reaktionszeiten zu verbessern und Übertragungsbandbreiten einzusparen.

11 Empfehlung des Rates vom 12. Juli 1999 zur Begrenzung der Exposition der Bevölkerung gegenüber elektromagnetischen Feldern (0 Hz–300 GHz) (1999/519/EG).

12 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 (NIS-Richtlinie). Die NIS-Kooperationsgruppe wurde durch die NIS-Richtlinie eingerichtet, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den EU-Mitgliedstaaten im Bereich der Cybersicherheit zu gewährleisten.

13 https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

Ergänzend zu diesem Bericht und als weitere Zuarbeit zu dem Instrumentarium erstellte die ENISA einen speziellen Bedrohungslagebericht[14] mit einer detaillierten Analyse bestimmter technischer Aspekte, insbesondere einer Aufstellung der Netzressourcen und ihrer Bedrohungen.

In dem Bericht über die EU-weit koordinierte Risikobewertung werden mehrere Aspekte hervorgehoben, die für 5G-Netze von Bedeutung sind, und zwar:

a) Die durch 5G-Technik eingeleiteten technischen Veränderungen werden die Gesamtangriffsfläche und die Zahl der möglichen Angriffspunkte erhöhen:

– Wegen der erweiterten Funktionen am Rand des Netzes und einer weniger zentralisierten Architektur als in früheren Generationen von Mobilfunknetzen werden einige Kernnetzfunktionen möglicherweise in andere Netzteile integriert, wodurch die betreffenden Ausrüstungen anfälliger werden (z. B. Basisstationen oder MANO-Funktionen).

– Der zunehmende Anteil von Software in 5G-Ausrüstungen führt zu erhöhten Risiken in den Prozessen der Softwareentwicklung und -aktualisierung, schafft neue Risiken von Konfigurationsfehlern und macht die Entscheidungen, die jeder Mobilfunknetzbetreiber in seiner Sicherheitsanalyse für die Aufbauphase des Netzes trifft, umso wichtiger.

b) Durch diese neuen technischen Merkmale gewinnt die Abhängigkeit der Mobilfunknetzbetreiber von Drittanbietern und ihre Rolle in der 5G-Lieferkette an Bedeutung.

Dadurch wiederum erhöht sich nicht nur die Zahl der Angriffswege, die von Angreifern, insbesondere von Akteuren, die von Nicht-EU-Staaten geführt oder unterstützt werden, gewählt werden könnten, weil sie in der Lage sind (Vorsatz und Mittel), Angriffe auf Telekommunikationsnetze von EU-Mitgliedstaaten durchzuführen, sondern auch die mögliche Schwere der Auswirkungen solcher Angriffe.

Vor diesem Hintergrund einer zunehmenden Verwundbarkeit durch Angriffe, die über Drittanbieter ermöglicht werden, bekommt das individuelle Risikoprofil der Anbieter eine ganz besondere Bedeutung, vor allem, wenn ein Anbieter in bestimmten Netzen oder Gebieten in erheblichem Umfang präsent ist.

c) Eine große Abhängigkeit von einem einzigen Anbieter erhöht die Gefahr und die Folgen eines möglichen Ausfalls dieses Anbieters. Dadurch verschärfen sich auch die potenziellen Folgen von Schwachstellen und Anfälligkeiten und deren möglicher Ausnutzung durch Angreifer, insbesondere bei einer Abhängigkeit von einem Anbieter, der ein hohes Risiko aufweist.

d) Sollten einige der neuen Einsatzmöglichkeiten, die für 5G geplant sind, tatsächlich verwirklicht werden, so werden 5G-Netze für viele kritische IT-Anwendungen letztlich zu einem wichtigen Bestandteil der Lieferkette. Dies hat jedoch nicht nur Folgen für die Anforderungen an die Vertraulichkeit und den Datenschutz. Vielmehr werden auch die

[14] *ENISA Threat landscape for 5G networks* (ENISA-Bedrohungslage für 5G-Netze): https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

Integrität und Verfügbarkeit dieser Netze zu wichtigen nationalen Sicherheitsbedenken und aus Sicht der EU zu einer großen sicherheitspolitischen Herausforderung.

Quelle: EU-weit koordinierte Risikobewertung

Aus dem Bericht über die EU-weit koordinierte Risikobewertung geht ferner hervor, dass diese Probleme zu einem neuen Sicherheitsparadigma führen, das eine Überprüfung des für den 5G-Sektor und sein Ökosystem derzeit geltenden politischen und sicherheitspolitischen Rahmens erforderlich macht und es unerlässlich erscheinen lässt, dass die Mitgliedstaaten die erforderlichen Risikominderungsmaßnahmen ergreifen.

Zur effektiven Bewältigung der festgestellten Risiken und zur Steigerung der Sicherheit und Widerstandsfähigkeit der 5G-Netze wird ein umfassendes Konzept benötigt, das eine Reihe von Schlüsselmaßnahmen mit zugehörigen Unterstützungsmaßnahmen umfasst, mit denen die Risiken gleichzeitig angegangen werden können. Die EU-weit koordinierte Risikobewertung lieferte die Grundlage für die Ermittlung von Risikominderungsmaßnahmen, die auf nationaler und europäischer Ebene ergriffen werden können.

In seinen Schlussfolgerungen vom 3. Dezember 2019 billigte der Rat die Ergebnisse der koordinierten Risikobewertung und betonte, „wie wichtig ein abgestimmter Ansatz und die wirksame Umsetzung der Empfehlung sind, wenn eine Fragmentierung im Binnenmarkt vermieden werden soll“[15]. In dieser Hinsicht forderte der Rat die Mitgliedstaaten, die Kommission und die ENISA auf, „im Rahmen ihrer Zuständigkeiten … alle erforderlichen Maßnahmen zu ergreifen, um die Sicherheit und die Integrität der elektronischen Kommunikationsnetze, insbesondere der 5G-Netze, zu gewährleisten, und weiter auf die Konsolidierung eines abgestimmten Ansatzes zur Bewältigung der mit den 5G-Technologien verbundenen sicherheitstechnischen Herausforderungen hinzuarbeiten“.

4. Das EU-Instrumentarium für die 5G-Cybersicherheit

Am 29. Januar 2020 veröffentlichte die NIS-Kooperationsgruppe das EU-Instrumentarium der Risikominderungsmaßnahmen[16]. Es erfasst alle Risiken, die im Bericht über die koordinierte Risikobewertung genannt wurden.

Das EU-Instrumentarium enthält die Aufstellung und Beschreibung einer Reihe strategischer und technischer Maßnahmen, die zur Minderung der festgestellten Risiken ergriffen werden können, samt zugehöriger Unterstützungsmaßnahmen zur Erhöhung ihrer Wirksamkeit. **Strategische Maßnahmen** sind Maßnahmen in Bezug auf erweiterte Regulierungsbefugnisse der Behörden zur Kontrolle der Beschaffung und des Ausbaus der Netze, besondere Maßnahmen zur Bewältigung von Risiken im Zusammenhang mit nichttechnischen Schwachstellen sowie mögliche Initiativen zur Förderung einer tragfähigen und diversifizierten 5G-Liefer- und Wertschöpfungskette, um systemische Abhängigkeitsrisiken langfristig zu vermeiden. **Technische Maßnahmen** sind Maßnahmen zur Erhöhung der Sicherheit von 5G-Netzen und -Ausrüstungen, durch die Risiken angegangen werden, die sich

[15] Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G (3.12.2019, 14517/19): https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/de/pdf.

[16] *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures* (Cybersicherheit von 5G-Netzen – EU-Instrumentarium der Risikominderungsmaßnahmen), 29. Januar 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

aus der Technik, den Prozessen sowie menschlichen und physikalischen Faktoren ergeben. Ferner enthält es **Risikominderungspläne** mit den jeweils wirksamsten Maßnahmen für alle in der EU-weit koordinierten Risikobewertung ermittelten Risikobereiche.

Wie in den von der NIS-Kooperationsgruppe vereinbarten Schlussfolgerungen zum EU-Instrumentarium empfohlen, gehört dazu unter anderem eine Reihe von **Schlüsselmaßnahmen**, die von allen Mitgliedstaaten und der Kommission wie folgt umzusetzen sind:

Schlussfolgerungen zum EU-Instrumentarium

Das EU-Instrumentarium enthält eine Reihe von Maßnahmen und Aktionen, die – wenn sie angemessen kombiniert und wirksam umgesetzt werden – die Grundlage für ein koordiniertes Vorgehen in diesem Bereich bilden. Angesichts des breiten Spektrums von Risikobereichen, die bei der EU-weit koordinierten Risikobewertung ermittelt wurden, und ihres unterschiedlichen Charakters wird keine einzige Art von Maßnahme ausreichen, sondern vielmehr eine Reihe von Maßnahmen in einer geeigneten Kombination erforderlich sein, um alle wichtigen Risikobereiche anzugehen.

Auf der Grundlage der Bewertung möglicher Risikominderungspläne und der Ermittlung der wirksamsten Maßnahmen wird in diesem Instrumentarium Folgendes empfohlen:

1. Alle Mitgliedstaaten sollten sicherstellen, dass sie über Maßnahmen verfügen (einschließlich der Befugnisse der nationalen Behörden), um angemessen und verhältnismäßig auf die derzeit bestehenden und künftigen Risiken zu reagieren, insbesondere sollten sie dafür sorgen, dass sie in der Lage sind, auf der Grundlage eines risikobasierten Ansatzes bestimmte Anforderungen oder Bedingungen für die Bereitstellung, den Ausbau und den Betrieb von 5G-Netzausrüstungen auf der Grundlage einer Reihe von Sicherheitserwägungen zu beschränken, zu verbieten und/oder vorzuschreiben.

Sie sollten insbesondere

- *die **Sicherheitsanforderungen** für Mobilfunknetzbetreiber verschärfen (z. B. strenge Zugangskontrollen, Vorschriften für sicheren Betrieb und sichere Überwachung, Beschränkungen für die Auslagerung bestimmter Funktionen usw.);*

- *die Risikoprofile der Anbieter bewerten und in der Folge **auf Anbieter, die als mit einem hohen Risiko behaftet gelten, einschlägige Beschränkungen anwenden, darunter den Ausschluss von Anbietern zur wirksamen Minderung der Risiken für wichtige Anlagen und Einrichtungen**, die in der EU-weit koordinierten Risikobewertung als kritisch und anfällig eingestuft wurden (z. B. Kernnetzfunktionen, Netzverwaltungs- und -koordinierungsfunktionen sowie Zugangsnetzfunktionen);*

- *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**, für ein angemessenes Gleichgewicht zwischen den Anbietern auf nationaler Ebene sorgen und eine **Abhängigkeit von Anbietern vermeiden, die als mit einem hohen Risiko behaftet gelten**; dazu muss auch die Bindung („lock-in“) an einen einzigen Anbieter vermieden werden, unter anderem durch die Förderung einer größeren Interoperabilität der Ausrüstungen.*

2. Die Europäische Kommission sollte gemeinsam mit den Mitgliedstaaten zu Folgendem beitragen:

- *Aufrechterhaltung einer **vielfältigen und zukunftsträchtigen 5G-Lieferkette**, um eine langfristige Abhängigkeit zu vermeiden, unter anderem durch*

  - *die umfassende Nutzung der bestehenden Werkzeuge und Instrumente der EU, insbesondere durch die Überprüfung **ausländischer Direktinvestitionen** mit potenziellen Auswirkungen auf wichtige 5G-Anlagen und -Einrichtungen und durch die Vermeidung von **Verzerrungen** auf dem 5G-Zuliefermarkt aufgrund von potenziellem Dumping oder möglichen Subventionen;*

  - *die weitere Stärkung der **Kapazitäten der EU im Bereich der 5G-Technik und deren Folgetechnik** durch Nutzung der einschlägigen EU-Programme und -Fördermittel;*

- *Erleichterung der Koordinierung zwischen den Mitgliedstaaten im Bereich der **Normung**, um spezifische Sicherheitsziele zu erreichen, und Entwicklung **einschlägiger EU-weiter Zertifizierungssysteme**, um sicherere Produkte und Verfahren zu fördern.*

3. Um sicherzustellen, dass sich dieses koordinierte Vorgehen bewähren kann, sollten das Mandat der NIS-Kooperationsgruppe und die Zusammenarbeit mit anderen einschlägigen Gremien und Stellen ausgeweitet werden, um insbesondere Folgendes zu erreichen:

- *regelmäßige Überprüfung der **nationalen und EU-Risikobewertungen** zur Sicherheit von 5G-Netzen und deren Folgenetzen mit Unterstützung der Kommission und der ENISA, weitere Ausarbeitung und Angleichung der angewandten Bewertungsmethodik und Anpassung an die sich entwickelnde 5G-Technik;*

- *Durchführung einer detaillierten und regelmäßigen **Überwachung und Bewertung der Umsetzung** des Instrumentariums auf Grundlage einer strukturierten Berichterstattung durch die Mitgliedstaaten;*

- *Koordinierung und Unterstützung der Durchführung **unterstützender Maßnahmen**, die eine Zusammenarbeit auf EU-Ebene erfordern, insbesondere im Hinblick auf die Ausarbeitung von Leitlinien und den Austausch bewährter Verfahren für die verschiedenen Maßnahmen;*

- *gegebenenfalls weitere Unterstützung einer möglichen Koordinierung auf EU-Ebene, insbesondere um für eine weitere Annäherung **im Hinblick auf die technischen und organisatorischen Sicherheitsanforderungen an Netzbetreiber** zu sorgen.*

Quelle: EU-Instrumentarium.

Die Schlussfolgerungen zum Instrumentarium zeigen, dass die Mitgliedstaaten entschlossen sind, gemeinsam auf die mit den 5G-Technologien verbundenen sicherheitstechnischen Herausforderungen zu reagieren. Dies ist von grundlegender Bedeutung für die Sicherheit in den Mitgliedstaaten und EU-weit, für die nationalen Volkswirtschaften sowie für den EU-Binnenmarkt und die technologische Unabhängigkeit Europas. Sowohl die EU-weit koordinierte Risikobewertung als auch das EU-Instrumentarium zeigen, wie wertvoll die gemeinsame Arbeit in der NIS-Kooperationsgruppe dank der intensiven Zusammenarbeit zwischen Vertretern aller Mitgliedstaaten, der Kommission und der ENISA ist.

Das Instrumentarium ermöglicht ein gemeinsames Vorgehen bei der 5G-Cybersicherheit, das die Kohärenz im gesamten Binnenmarkt durch EU-politische Maßnahmen und Koordinierung sowie die Ausübung der Zuständigkeiten der Mitgliedstaaten, insbesondere im Hinblick auf die nationale Sicherheit, fördert. Die darin enthaltenen Risikominderungsmaßnahmen und -pläne ermöglichen eine angemessene, wirksame und verhältnismäßige Reaktion der EU auf die gemeinsamen Herausforderungen im Bereich der 5G-Cybersicherheit.

Die Kommission begrüßt die Veröffentlichung des EU-Instrumentariums für die 5G-Cybersicherheit und unterstützt alle oben genannten Schlussfolgerungen uneingeschränkt.

Die Kommission fordert die Mitgliedstaaten und die einschlägigen Organe, Agenturen und sonstigen Einrichtungen der Union auf,

i) für die rasche Umsetzung wirksamer und geeigneter Strategien zur Risikominderung im Einklang mit dem EU-Instrumentarium in der gesamten EU zu sorgen und

ii) alle erforderlichen weiteren Maßnahmen zu treffen, um die Koordinierung auf Unionsebene zu gewährleisten, unter anderem durch die Fortsetzung der Arbeiten innerhalb der NIS-Kooperationsgruppe und die Einrichtung eines robusten Mechanismus zur Überwachung der Umsetzung des EU-Instrumentariums, sodass die Wirksamkeit der Maßnahmen und das reibungslose Funktionieren des Binnenmarkts gewährleistet wird.

5. Umsetzung des Instrumentariums

Die Entschlossenheit der Mitgliedstaaten, das Instrumentarium vollumfänglich zu nutzen, ist für ein glaubwürdiges und erfolgreiches europäisches Vorgehen bei der 5G-Sicherheit von entscheidender Bedeutung. Die Mitgliedstaaten werden zwar auf Grundlage der nationalen Gegebenheiten zu entscheiden haben, ob eine bestimmte Maßnahme geeignet ist, es ist aber unbedingt notwendig, eine **Reihe von Schlüsselmaßnahmen entsprechend den Empfehlungen der NIS-Kooperationsgruppe (siehe Schlussfolgerungen zum Instrumentarium) in jedem Mitgliedstaat und einige auf EU-Ebene einzuführen**, um den ermittelten Risiken zu begegnen.

Die Kommission ist bereit, in den nächsten Phasen weiterhin uneingeschränkt Unterstützung zu leisten, und ruft die Mitgliedstaaten auf,

– **bis zum 30. April 2020** konkrete und messbare Schritte zur Umsetzung der in den Schlussfolgerungen zum EU-Instrumentarium empfohlenen Schlüsselmaßnahmen zu unternehmen;

– **bis zum 30. Juni 2020** auf der Grundlage der regelmäßigen Berichterstattung und Überwachung, die mit Unterstützung der Kommission und der ENISA insbesondere im Rahmen der NIS-Kooperationsgruppe stattfindet, einen Bericht der NIS-Kooperationsgruppe über den Stand der Umsetzung dieser Schlüsselmaßnahmen in den einzelnen Mitgliedstaaten vorzubereiten.

5.1. Ein risikobasierter, abgestimmter Ansatz für 5G-Anbieter

Angesichts des übergeordneten Ziels, die Sicherheit und Widerstandsfähigkeit der 5G-Netze und ihre Zukunftsfähigkeit zu gewährleisten, waren sich die Mitgliedstaaten darin einig, dass die Risikoprofile einzelner Anbieter bewertet und in der Folge entsprechende

Beschränkungen auf Anbieter angewendet werden müssen, die als mit einem hohen Risiko behaftet gelten, darunter der Ausschluss von Anbietern, wo dies – entsprechend dem Instrumentarium – zur wirksamen Minderung der Risiken für wichtige Anlagen und Einrichtungen erforderlich ist. Die Kommission ist bereit, die Mitgliedstaaten bei der Umsetzung dieser Maßnahmen zu unterstützen.

Zur Unterstützung ihrer EU-weiten Umsetzung bieten die EU-weit koordinierte Risikobewertung und das EU-Instrumentarium Orientierungshilfen in Bezug auf 1) die Bewertung der Risikoprofile von Anbietern[17] und 2) die Sensibilität von Netzelementen und -funktionen[18] sowie weiterer Anlagen und Einrichtungen. Sowohl die EU-weit koordinierte Risikobewertung als auch die Maßnahmen im Rahmen des Instrumentariums erfassen die Risiken, die mit den Anbietern von 5G-Netzausrüstungen und -Netzdiensten verbunden sind. Sie betreffen jedoch keine anderen Produkte oder Dienstleistungen, die diese oder andere Anbieter möglicherweise bereitstellen.

Gemäß Abschnitt 2.37 der EU-weit koordinierten Risikobewertung können die Risikoprofile einzelner Anbieter anhand mehrerer Faktoren bewertet werden.

Die Bewertung der Risikoprofile der Anbieter sollte ausschließlich aus Sicherheitsgründen und auf der Grundlage objektiver Kriterien erfolgen. Um ein koordiniertes Vorgehen bei der Umsetzung dieser Maßnahmen zu erleichtern, wird den Mitgliedstaaten im Instrumentarium empfohlen, Informationen über nationale Ansätze und bewährte Verfahren auszutauschen. Darüber hinaus ist die Kommission der Auffassung, dass diese Maßnahme eine der ersten Prioritäten der nächsten Phase der Arbeiten der NIS-Kooperationsgruppe in Zusammenarbeit mit der Kommission und der ENISA sein sollte.

Es ist wichtig, dass Maßnahmen zur Beschränkung von Anbietern, die als mit einem hohen Risiko behaftet gelten, darunter der Ausschluss von Anbietern zur wirksamen Risikominderung, sowie Maßnahmen zur Vermeidung der Abhängigkeit von diesen Anbietern rechtzeitig getroffen werden. Wenn dies so früh wie möglich, auch bei 5G-Frequenzlizenzverfahren, geschieht, erhöht das die Vorhersehbarkeit für die Marktteilnehmer, sodass diese zu einer raschen Einführung der 5G-Netze beigetragen und die langfristige Sicherheit der 5G-Netze und die Widerstandsfähigkeit der 5G-Lieferkette gewährleistet wird.

Gleichzeitig können für die Umsetzung dieser Maßnahmen auf nationaler Ebene – soweit erforderlich und gerechtfertigt – unterschiedliche Zeitpläne festgelegt werden, insbesondere wenn ein hohes Maß an Abhängigkeit von Ausrüstungen oder Diensten von Anbietern besteht, die als mit einem hohen Risiko behaftet gelten (z. B. durch Berücksichtigung von Modernisierungszyklen der Ausrüstung, insbesondere bei der Migration von „nicht eigenständigen“ zu „eigenständigen“ 5G-Netzen). Die Mitgliedstaaten könnten die Festlegung von Umsetzungsplänen mit angemessenen Übergangszeiträumen für die betroffenen Netzbetreiber in Erwägung ziehen. In diesem Zusammenhang sollten Übergangszeiträume so festgelegt werden, dass im Einklang mit den Zielen des 5G-Aktionsplans[19] die Anreize für

[17] Abschnitt 2.37 der EU-weit koordinierten Risikobewertung.

[18] In Abschnitt 2.21 der EU-weit koordinierten Risikobewertung werden die wichtigsten Kategorien von Elementen und Funktionen und ihr Gesamtanfälligkeitsgrad sowie eine Reihe von Schlüsselelementen aufgeführt, die von den Mitgliedstaaten für jede Kategorie ermittelt wurden. In den Abschnitten 2.28 und 2.29 wird eine Reihe anderer Arten anfälliger Anlagen und Einrichtungen oder Bereiche (z. B. spezifische Einrichtungen oder geografische Gebiete) genannt.

[19] COM(2016) 588 vom 14.9.2016: Mitteilung der Kommission „5G für Europa: ein Aktionsplan“.

Investitionen in moderne Netzausrüstungen erhalten oder sogar verstärkt werden, einschließlich der beschleunigten Einführung vollwertiger („eigenständiger“) 5G-Kernnetze und der Ersetzung bestehender 4G-Ausrüstungen in anderen Teilen der Netze (z. B. im Funkzugangsnetz).

Aufgrund der Komplexität der softwaregestützten 5G-Netze werden Telekommunikationsbetreiber darüber hinaus möglicherweise zunehmend auf Dritte angewiesen sein, um neben der Bereitstellung von Netzausrüstung bestimmte Aufgaben wie die Wartung und Modernisierung der 5G-Netze und -Software sowie andere ausgelagerte verwaltete Dienste auszuführen. Wie in der EU-weit koordinierten Risikobewertung beschrieben, stellt dies ein erhebliches Sicherheitsrisiko dar. Diesem Aspekt sollte daher besondere Aufmerksamkeit gewidmet werden. Auch die Risikoprofile der mit diesen Diensten betrauten Anbieter müssen unbedingt einer gründlichen Sicherheitsbewertung unterzogen werden, insbesondere wenn diese Aufgaben nicht in der EU ausgeführt werden. Um die langfristige Integrität der 5G-Infrastruktur zu wahren, sollten geeignete Maßnahmen ergriffen werden, einschließlich der Anwendung von Beschränkungen insbesondere in sensiblen Teilen der 5G-Netze oder des erforderlichen Ausschlusses von mit hohem Risiko behafteten Anbietern im Einklang mit den Risikominderungsmaßnahmen des Instrumentariums.

5.2. Die unterstützende Rolle der Kommission bei Umsetzung des Instrumentariums

Die Kommission wird weiterhin die Umsetzung des EU-Konzepts für die 5G-Cybersicherheit im Allgemeinen unterstützen und spezifische Initiativen in Bezug auf Maßnahmen und Ziele des Instrumentariums ergreifen, wo dadurch ein Mehrwert erzielt werden kann. Die Kommission wird ihre Befugnisse und einschlägigen Instrumente in vollem Umfang nutzen, soweit dies erforderlich ist, um die ermittelten Sicherheitsbedenken auszuräumen. Auf diese Weise und durch gemeinsames Handeln mit den Mitgliedstaaten und dem Privatsektor will die Kommission ein strategisches Vorgehen unterstützen, das dazu beitragen wird, die technologische Unabhängigkeit und Führungsrolle der EU bei der künftigen Entwicklung von Netztechnik, Cybersicherheitstechnik und allen relevanten Bausteinen, von denen unsere gesamte Wirtschaft und Sicherheit abhängen, zu gewährleisten.

Die Kommission wird insbesondere folgende Maßnahmen ergreifen, um die Umsetzung der entsprechenden Risikominderungsmaßnahmen im Rahmen des Instrumentariums in den in ihre Zuständigkeit fallenden Bereichen sicherzustellen:

Gewährleistung der Cybersicherheit von 5G-Netzen und einer vielfältigen 5G-Wertschöpfungskette:

– Zusammenarbeit auf dem Gebiet der Cybersicherheit: weitere Unterstützung der Mitgliedstaaten bei der wirksamen, koordinierten und zeitnahen Umsetzung nationaler Maßnahmen durch die NIS-Kooperationsgruppe;

– Telekommunikations- und Cybersicherheitsvorschriften: Unterstützung der Umsetzung von Maßnahmen des Instrumentariums in Bezug auf Sicherheitsanforderungen, insbesondere im Hinblick auf die einschlägigen Bestimmungen im Rahmen der europäischen Vorschriften für die elektronische Kommunikation, und Prüfung des Mehrwerts möglicher Durchführungsrechtsakte, in denen die technischen und organisatorischen Sicherheitsmaßnahmen im Einzelnen festgelegt werden, um die nationalen Vorschriften zu ergänzen und die Wirksamkeit und Kohärenz der den Betreibern auferlegten Sicherheitsmaßnahmen zu verbessern;

– **Normung**: Maßnahmen zur Aufrechterhaltung und – wo nötig – Intensivierung der europäischen Beteiligung an den jeweiligen Normungsgremien, damit die Ziele Europas in den Bereichen Sicherheit und Interoperabilität erreicht werden. Insbesondere wird die Kommission gemeinsam mit den Mitgliedstaaten die technischen Spezifikationen und Normen bewerten und fördern, die die Interoperabilität zwischen den Anbietern von 5G-Ausrüstungen in verschiedenen Teilen des Netzes, einschließlich herkömmlicher Netze, ermöglichen, um beispielsweise mithilfe offener interoperabler Schnittstellen ein echtes herstellerneutrales Umfeld zu schaffen;

– **Zertifizierung**: Unterstützung der Entwicklung von 5G-Zertifizierungssystemen, die den Bedürfnissen von 5G-Netzen im Rahmen des EU-Zertifizierungsrahmens für die Cybersicherheit gerecht werden;

– **Überprüfung ausländischer Direktinvestitionen**: Unterstützung der Umsetzung des EU-Überprüfungsrahmens durch eine Erfassung der 5G-Wertschöpfungskette, einschließlich anfälliger Netzressourcen, und eine regelmäßige Überwachung ausländischer Direktinvestitionen entlang der Wertschöpfungskette. Entsprechend dem Zeitplan für die Überprüfung ausländischer Direktinvestitionen (ab Oktober 2020) wird die Kommission ausländische Investitionen im 5G-Bereich im Einklang mit den Vorgaben der Verordnung (EU) 2019/452 prüfen und dabei die EU-weit koordinierte Risikobewertung und das EU-Instrumentarium berücksichtigen;

– **handelspolitische Schutzinstrumente**: Überwachung aller relevanten Marktentwicklungen in der EU und in Drittländern sowie Schutz der EU-Akteure auf dem europäischen 5G-Markt durch handelspolitische Schutzmaßnahmen gegen potenzielle handelsverzerrende Praktiken (Dumping oder Subventionierung), gegebenenfalls auch durch Einleitung von Voruntersuchungen;

– **Wettbewerbsregeln:** Überwachung des Funktionierens der Märkte für 5G-Hard- und -Software, um sicherzustellen, dass diese Märkte wettbewerbsorientierte Ergebnisse hervorbringen, auch in Bezug auf eine mögliche vertragliche oder technische Bindung („*lock-in*“);

– **EU-Förderprogramme**: Gewährleistung, dass die Beteiligung an EU-Finanzierungsprogrammen in den einschlägigen Technologiebereichen von der Einhaltung der Sicherheitsanforderungen abhängig gemacht wird, indem die Sicherheitsbedingungen in den FuI-Programmen, insbesondere im Programm „Horizont Europa“, im Programm „Digitales Europa“ und in der Fazilität „Connecting Europe 2“, in den europäischen Struktur- und Investitionsfonds und in anderen einschlägigen Programmen umfassend genutzt und weiterhin angewandt werden. Ein ähnlicher Ansatz sollte auch bei den externen Finanzierungsprogrammen und Finanzierungsinstrumenten der EU verfolgt werden, auch im Hinblick auf die Förderung durch internationale Finanzinstitute;

– **Öffentliche Aufträge:** Nutzung der Vergabe öffentlicher Aufträge im Bereich 5G-Netze, um die festgelegten Ziele Sicherheit, Anbietervielfalt und langfristige Nachhaltigkeit von 5G-Netzen zu unterstützen; insbesondere ist darauf hinzuwirken, dass Sicherheitsaspekte bei der Vergabe öffentlicher Aufträge im Bereich der 5G-Netze im Einklang mit den EU-Vorschriften für die Vergabe öffentlicher Aufträge gebührend berücksichtigt werden;

– Reaktion auf Sicherheitsvorfälle und Krisenmanagement (Konzeptentwurf) und Cyberübungen: Umfassende Nutzung der Entwicklung des EU-Konzeptentwurfs[20] für die koordinierte Reaktion auf große Cybersicherheitsvorfälle. Außerdem ist gemeinsam mit der ENISA zu prüfen, ob eine 5G-Cyberübung durchgeführt werden kann, sobald die Marktreife dies zulässt.

Und unter der Verantwortung des Hohen Vertreters der Union für Außen- und Sicherheitspolitik und Vizepräsidenten der Kommission und des Rates:

– Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten (Instrumentarium für die Cyberdiplomatie)[21]: Die Mitgliedstaaten werden ermuntert, im Falle böswilliger Cyberaktivitäten, die die Integrität und Sicherheit der EU bedrohen, die einschlägigen Maßnahmen der Gemeinsamen Außen- und Sicherheitspolitik, die Teil des EU-Instrumentariums für die Cyberdiplomatie sind (gegebenenfalls einschließlich restriktiver Maßnahmen), zu nutzen, um die Zusammenarbeit zu fördern, Bedrohungen einzudämmen und Einfluss auf das Verhalten potenzieller Angreifer zu nehmen.

Darüber hinaus wird eine Reihe von Programmen dazu beitragen, das Risiko einer langfristigen Abhängigkeit zu vermeiden oder zu begrenzen, indem – im Einklang mit den internationalen Verpflichtungen der EU – ein diversifizierter und nachhaltiger Markt für 5G gefördert wird, unter anderem auch durch den Erhalt der EU-Kapazitäten in der 5G-Wertschöpfungskette und durch Investitionen in Innovation.

Förderung von Innovation und Investitionen in Cybersicherheit und Netzinfrastrukturtechnik:

– EU-**Förderprogramme**: Erhöhung der Investitionen in Forschung, Innovation und Einführung von Netztechnik und einschlägigen Grundbausteinen. Die Kommission hat vorgeschlagen, im EU-Haushalt 2021-2027 knapp 3 Mrd. EUR für Cybersicherheitstechnik vorzusehen. Dies schließt Investitionen in Forschung und Innovation im Rahmen des Programms „Horizont Europa“ und Unterstützung von Cybersicherheitskapazitäten im Rahmen des Programms „Digitales Europa“ ein. Aus dem Programm „InvestEU“ kann ebenfalls finanzielle Unterstützung für Forschung und Entwicklung im Bereich 5G und für die 5G-Einführung geleistet werden.

Darüber hinaus schlägt die Kommission vor, im Rahmen des nächsten „Horizont Europa“-Programms[22] in Partnerschaft mit der Industrie und in Abstimmung mit den Mitgliedstaaten eine institutionalisierte europäische Partnerschaft für das Internet der nächsten Generation/6G („Intelligente Netze und Dienste“) einzurichten, um den 5G-Ausbau abzuschließen und vor allem die **Vorbereitungen für 6G**, die Mobilfunktechnologie der nächsten Generation vorzubereiten, zu treffen. Hierfür wurden Investitionen in Höhe von mehr als 2,5 Mrd. EUR aus dem EU-Haushalt 2021-2027 vorgeschlagen, ergänzt durch private Investitionen in Höhe von mindestens 7,5 Mrd. EUR.

[20] Empfehlung (EU) 2017/1584 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

[21] Schlussfolgerungen des Rates vom 20. November 2017, 9916/17.

[22] Mittel können auch aus der CEF 2.0 und dem Programm „Digitales Europa“ bereitgestellt werden.

– **Industrielle Entwicklung und Einführung**: Bewertung von Marktlücken oder Marktversagen entlang der 5G-Wertschöpfungskette, die gezielte Maßnahmen im Rahmen des nächsten langfristigen Haushalts oder eines möglichen, nach den Vorschlägen des hochrangigen IPCEI-Forums aufgestellten „Wichtigen Projekts von gemeinsamem europäischem Interesse“ (IPCEI) zur Cybersicherheit rechtfertigen würden. Die Entscheidung, IPCEI zu konzipieren und aufzustellen, liegt bei den Mitgliedstaaten und den Unternehmen. Die EU-Vorschriften schaffen günstige Rahmenbedingungen, und die Kommission kann bei der Herstellung der notwendigen Kontakte helfen und Orientierungshilfen geben.

6. Schlussfolgerungen

5G-Netze werden den Bürgerinnen und Bürgern, der Gesellschaft und der Wirtschaft in Europa vielfältige Chancen eröffnen. Die Gewährleistung der Sicherheit und Widerstandsfähigkeit der 5G-Netze ist daher von größter Bedeutung. Gleichzeitig stellen Cybersicherheitsbedrohungen (einschließlich der Gefahr von Eingriffen durch Drittstaaten oder von Drittstaaten unterstützte Akteure) eine wachsende Herausforderung dar, die neben der zunehmenden Abhängigkeit von Technologien und Daten immer mehr an Bedeutung gewinnt. Die Cybersicherheit zu vernachlässigen, würde das Vertrauen in die Entwicklung der digitalen Wirtschaft und Gesellschaft untergraben und verhindern, dass die EU die Vorteile dieser Entwicklung in vollem Umfang ausschöpft. All dies macht eine kontinuierlich angepasste und intensivierte Reaktion erforderlich.

Ein koordiniertes und kohärentes EU-Cybersicherheitskonzept für kritische Technologien und Netze ist eine Voraussetzung dafür, dass die EU ihre technologische Souveränität wahren und ihre industriellen Kapazitäten erhalten und ausbauen kann. Die Kommission wird die Umsetzung des EU-Cybersicherheitskonzepts für 5G-Netze voll und ganz unterstützen und gleichzeitig sicherstellen, dass die EU-Märkte weiterhin offen bleiben für Produkte und Dienste, die die immer höheren Anforderungen an Cybersicherheit und Vertrauenswürdigkeit erfüllen.

Hierfür ist es wichtig, dass sich alle Beteiligten weiterhin für 5G-Sicherheit stark machen, was auch eine kontinuierliche Zusammenarbeit zwischen den Mitgliedstaaten, der Kommission und der ENISA erfordern wird.

Als sofortigen nächsten Schritt fordert die Kommission, wie oben dargelegt, die Mitgliedstaaten auf, nun rasch tätig zu werden, um die als Teil des Instrumentariums vereinbarten Maßnahmen wirksam und objektiv umzusetzen, und mit Unterstützung der Kommission und der ENISA weiter zusammenzuarbeiten, um die Koordinierung auf EU-Ebene sicherzustellen. Parallel hierzu wird die Kommission alle einschlägigen Maßnahmen in ihrem Zuständigkeitsbereich auf den Weg bringen, um die Umsetzung des Instrumentariums durch die Mitgliedstaaten zu unterstützen und seine Wirkung zu verstärken.

Anlage: Risikokategorien (Quelle: EU-weit koordinierte Risikobewertung)

	Risikokategorien
Risikoszenarien im Zusammenhang mit unzureichenden Sicherheitsmaßnahmen	*R1: Fehlkonfiguration von Netzen*
	R2: Mangelnde Zugangskontrolle
Risikoszenarien im Zusammenhang mit der 5G-Lieferkette	*R3: Schlechte Produktqualität*
	R4: Abhängigkeit von einem einzelnen Anbieter innerhalb einzelner Netze oder mangelnde landesweite Vielfalt
Risikoszenarien im Zusammenhang mit der Vorgehensweise der wichtigsten Bedrohungsakteure	*R5: Staatliche Einflussnahme über die 5G-Lieferkette*
	R6: Nutzung von 5G-Netzen durch organisierte Kriminalität oder Verbrechergruppen, die es auf Endnutzer abgesehen haben
Risikoszenarien im Zusammenhang mit gegenseitigen Abhängigkeiten zwischen 5G-Netzen und anderen kritischen Systemen	*R7: Erhebliche Störung kritischer Infrastrukturen oder Dienste*
	R8: Massive Netzausfälle aufgrund einer Unterbrechung der Stromversorgung oder Störungen anderer Unterstützungssysteme
Risikoszenarien im Zusammenhang mit Geräten der Endnutzer	*R9: Ausnutzung des Internets der Dinge (IoT)*