



Rat der
Europäischen Union

005602/EU XXVII. GP
Eingelangt am 04/12/19

Brüssel, den 3. Dezember 2019
(OR. en)

14517/19

TELECOM 372
CYBER 323
COMPET 769
MI 815
CONSOM 320

BERATUNGSERGEBNISSE

Absender: Generalsekretariat des Rates

vom 3. Dezember 2019

Empfänger: Delegationen

Betr.: Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G
– Schlussfolgerungen des Rates (3. Dezember 2019)

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G, die der Rat (Verkehr, Telekommunikation und Energie) auf seiner Tagung vom 3. Dezember 2019 angenommen hat.

Schlussfolgerungen des Rates zur Bedeutung von 5G für die europäische Wirtschaft und zur Notwendigkeit der Begrenzung der Sicherheitsrisiken im Zusammenhang mit 5G

DER RAT DER EUROPÄISCHEN UNION

– unter Hinweis auf das Potenzial der 5G-Netze für die europäische Wirtschaft, den EU-Binnenmarkt und die europäischen Bürgerinnen und Bürger –

1. STELLT FEST, dass es sich bei 5G um eine Weiterentwicklung der 4G-Netze handelt und dass durch 5G das Potenzial für die Bereitstellung von Mobilfunkdiensten wächst, während zugleich in einer Vielzahl von Sektoren innovative Geschäftsmodelle und öffentliche Dienstleistungen entstehen und sich für die europäischen Bürgerinnen und Bürgern, Telekommunikationsbetreiber, Unternehmen einschließlich KMU, die öffentliche Hand sowie andere Interessenträgern noch weitere Chancen bieten können;
2. ERINNERT DARAN, dass die Union – beispielsweise mit der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation und der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) – einen Rechtsrahmen für die Bewältigung und Minderung von Cybersicherheitsrisiken im Zusammenhang mit 5G entwickelt hat;
3. STELLT FEST, dass die ehrgeizigen Ziele des 5G-Aktionsplans der Kommission von 2016, der Ministererklärung von Tallinn zu 5G sowie des damit verbundenen Fahrplans, den die Mitgliedstaaten 2017 ausgehend von den Zielvorgaben für die Gigabit-Gesellschaft vereinbart haben, erfüllt werden müssen;

4. BETONT, dass 5G-Netze Teil der wichtigen Infrastruktur für den Betrieb und die Aufrechterhaltung lebenswichtiger gesellschaftlicher und wirtschaftlicher Funktionen sowie einer breiten Palette von Diensten sein werden, die Voraussetzung für einen funktionierenden Binnenmarkt sowie dessen Digitalisierung sind, und UNTERSTREICHT in diesem Zusammenhang die Bedeutung der technologischen Souveränität Europas und der weltweiten Verbreitung des Ansatzes, den die EU im Hinblick auf die Cybersicherheit künftiger elektronischer Kommunikationsnetze verfolgt;
5. HEBT HERVOR, dass für einen zügigen, nachfrageorientierten Ausbau der 5G-Netze gesorgt werden muss und dass 5G ein Schlüsselfaktor für die europäische Wettbewerbsfähigkeit und Nachhaltigkeit, eine zentrale Voraussetzung für künftige digitale Dienste sowie eine Priorität für den europäischen Binnenmarkt ist; BETONT in diesem Zusammenhang auch, wie wichtig die Zusammenarbeit der Mitgliedstaaten bei der Verbreitung von 5G-Netzen in den Grenzgebieten zwischen Mitgliedstaaten ist;
6. STELLT FEST, dass die Öffentlichkeit für die Möglichkeiten von 5G sensibilisiert werden muss und die Kompetenzen innerhalb der Entwicklergemeinschaft und verschiedener Nutzergruppen erweitert werden müssen und dass die öffentliche Hand ihren Beitrag zur verstärkten Verbreitung von 5G leisten muss, indem sie mit gutem Beispiel vorangeht; BESTÄRKT alle einschlägigen Interessenträger darin, sich im Interesse des erfolgreichen Ausbaus von 5G am Austausch von Informationen und Erfahrungen zu beteiligen – auch zu Fragen im Zusammenhang mit der Bemessung der Grenzwerte für elektromagnetische Felder (EMF);
7. BESTÄRKT die Kommission und die Mitgliedstaaten darin, die notwendigen Schritte zu unternehmen, damit die EU zu einem führenden Markt für die Einführung von 5G-Netzen und die Entwicklung 5G-basierter Lösungen wird, die zu Wachstum und Innovation beitragen, den Alltag von Bürgerinnen und Bürgern sowie Unternehmen verbessern, neue Dienste und Anwendungen ermöglichen und in Schlüsselsektoren und -industrien wie Energiewirtschaft, Gesundheitsversorgung, Landwirtschaft, Finanzwesen und der Mobilitätsbranche für die gesamte Gesellschaft neue Möglichkeiten eröffnen;

– unter Hinweis auf die mit 5G-Netzen verbundenen Herausforderungen –

8. BETONT, dass die Sicherheit und Widerstandsfähigkeit elektronischer Kommunikationsnetze und -dienste, insbesondere in Bezug auf 5G, anhand eines risikobasierten Ansatzes gewahrt werden muss;
9. BETONT, dass die Einführung von 5G-Netzen zwar neue Möglichkeiten eröffnet, die EU und die Mitgliedstaaten aber – aufgrund der tiefgreifenden Veränderungen, die mit der 5G-Technologie für Netze, Geräte und Anwendungen verbunden sind, und der zunehmenden Sicherheitsbedenken, die nicht nur bezüglich Vertraulichkeit und Privatsphäre, sondern auch in Bezug auf die Integrität und die Verfügbarkeit von 5G-Netzen bestehen – ein besonderes Augenmerk auf die Förderung der Cybersicherheit dieser Netze sowie aller von elektronischer Kommunikation abhängiger Dienste richten müssen;
10. BEGRÜßT die Bemühungen um die Wahrung der Sicherheit von 5G-Netzen, die derzeit auf europäischer Ebene, insbesondere ausgehend von der Empfehlung der Kommission zur Cybersicherheit der 5G-Netze, gemeinsam unternommen werden, und BETONT, wie wichtig ein abgestimmter Ansatz und die wirksame Umsetzung der Empfehlung sind, wenn eine Fragmentierung im Binnenmarkt vermieden werden soll;
11. BEGRÜßT die am 9. Oktober 2019 veröffentlichte koordinierte Risikobewertung der EU als erstes vorweisbares Ergebnis seit der Empfehlung;
12. BETONT, dass die durch 5G bedingten technologischen Veränderungen zu einer Vergrößerung der Gesamtangriffsfläche führen werden, sodass in besonderem Maße auf die Risikoprofile einzelner Anbieter geachtet werden muss;
13. BETONT, dass es neben den technischen Risiken im Zusammenhang mit der Cybersicherheit von 5G-Netzen auch nichttechnische Faktoren zu berücksichtigen gilt, wozu beispielsweise die rechtlichen und politischen Rahmenbedingungen gehören, die für Anbieter in Drittländern gelten könnten;

14. BEKRÄFTIGT, wie wichtig es ist, dass die Mitgliedstaaten prüfen, ob eine Diversifizierung der Anbieter geboten ist, um eine allzu große Abhängigkeit von einem einzigen Anbieter zu vermeiden oder einzugrenzen, da der potenzielle Ausfall eines solchen Anbieters folgenschwerer wäre;
15. HEBT HERVOR, dass es die Risiken im Zusammenhang mit den wechselseitigen Abhängigkeiten zwischen 5G-Netzen und anderen kritischen öffentlichen und privaten Systemen und Diensten zu bewerten gilt;

WESHALB DER RAT

16. BETONT, dass ein zügiger und sicherer Ausbau der 5G-Netze die Voraussetzung für die Stärkung der Wettbewerbsfähigkeit der EU ist und einen abgestimmten Ansatz in der EU erfordert, wobei die Zuständigkeiten der Mitgliedstaaten in Fragen des Netzausbau und der nationalen Sicherheit davon nicht berührt werden;
17. HERVORHEBT, dass die Stärkung des Vertrauens in 5G-Technologien voll und ganz auf den Grundwerten der EU – wie Menschenrechte und Grundfreiheiten, Rechtsstaatlichkeit, Schutz der Privatsphäre, personenbezogener Daten und des geistigen Eigentums –, auf der Verpflichtung zu Transparenz, zu Zuverlässigkeit und zur Inklusion aller Interessenträger sowie Bürgerinnen und Bürger sowie auf der verstärkten internationalen Zusammenarbeit gründet;
18. UNTERSTREICHT, dass es aufgrund der immer komplexeren, zunehmend vernetzten, sich rasch entwickelnden Technologie erforderlich ist, einen umfassenden Ansatz zu verfolgen und als feste Bestandteile von 5G-Infrastruktur und Endgeräten wirksame und verhältnismäßige Sicherheitsmaßnahmen mit dem Schwerpunkt Sicherheit und eingebauter Datenschutz vorzusehen;
19. BETONT, dass 5G und andere damit verbundene elektronische Kommunikationsnetze während ihres gesamten Lebenszyklus kontinuierlich geschützt werden müssen, damit die gesamte Lieferkette und alle einschlägigen Ausrüstungen erfasst sind;

20. HERVORHEBT, dass potenzielle Probleme für die Strafverfolgung, die mit der Einführung von 5G-Netzen und -Diensten verbunden sind, entschärft und gelöst werden müssen, unter anderem etwa durch das rechtmäßige Abfangen von Daten;
21. FESTSTELLT, dass für alle einschlägigen Hersteller, Betreiber elektronischer Kommunikationsnetze und Diensteanbieter robuste gemeinsame Sicherheitsnormen und -maßnahmen eingeführt werden müssen, die internationalen Normungsbemühungen in Bezug auf 5G Rechnung tragen, und dass zentrale Komponenten, beispielsweise für die nationale Sicherheit wesentliche Komponenten, nur von vertrauenswürdigen Partnern bezogen werden dürfen;
22. die laufenden Arbeiten der Agentur der Europäischen Union für Cybersicherheit (ENISA) an dem europäischen Rahmen für die Cybersicherheitszertifizierung UNTERSTÜTZT, der mit dem Rechtsakt zur Cybersicherheit eingerichtet wurde und ein höheres Cybersicherheitsniveau bei IKT-Produkten, -Diensten und -Prozessen verspricht;
23. HERVORHEBT, dass bestimmte sicherheitstechnische Herausforderungen im Zusammenhang mit 5G-Netzen zwar durch Normung und Zertifizierung bewältigt werden könnten, zur wirksamen Minderung der Risiken aber zusätzliche Sicherheitsmaßnahmen erforderlich sind;
24. BEGRÜßT, dass die Kommission zurzeit in Zusammenarbeit mit den Mitgliedstaaten und der Privatwirtschaft an einer strategischen europäischen Partnerschaft für intelligente Netze und Dienste im Rahmen von Horizont Europa arbeitet, die der Förderung von Investitionen, der Erhaltung und Stärkung der Wettbewerbsfähigkeit, der Ausweitung von Forschung und Innovation sowie der Entwicklung sicherer Lösungen im Bereich 5G und darüber hinaus dienen soll;
25. die Priorisierung der Cybersicherheit in dem Vorschlag für ein Programm „Digitales Europa“ als Mittel zur Stärkung der Cybersicherheitskapazitäten der EU sowie die Initiative für grenzüberschreitende 5G-TEN-V-Korridore im Rahmen des vorgeschlagenen Programms für die Fazilität „Connecting Europe“ BEGRÜßT;

26. die Mitgliedstaaten und die Kommission AUFFORDERT, im Rahmen ihrer Zuständigkeiten mit der Unterstützung der ENISA 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 sowie ausgehend von den derzeitigen gemeinsamen Arbeiten am 5G-Sicherheitsinstrumentarium wirksame gemeinsame Methoden und Instrumente zur Minderung der mit 5G-Netzen verbundenen Risiken zu ermitteln.
-