Rat der
Europäischen Union

Brüssel, den 6. Juni 2025
(OR. en)

9953/25

TELECOM 180
CYBER 160
COMPET 496
MI 361
PROCIV 66

BERATUNGSERGEBNISSE

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	7929/25
Betr.:	Schlussfolgerungen zu einer zuverlässigen und resilienten Konnektivität – Schlussfolgerungen des Rates (6. Juni 2025)

Die Delegationen erhalten in der Anlage die Schlussfolgerungen des Rates zu einer zuverlässigen und resilienten Konnektivität, die der Rat (Verkehr, Telekommunikation und Energie) auf seiner Tagung vom 6. Juni 2025 gebilligt hat.

ANLAGE

Schlussfolgerungen des Rates zu einer zuverlässigen und resilienten Konnektivität

DER RAT DER EUROPÄISCHEN UNION —

UNTER HINWEIS AUF

- die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation,
- die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie),
- die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates,
- die Gemeinsame Mitteilung an das Europäische Parlament und den Rat über die Aktualisierung der EU-Strategie für maritime Sicherheit und des Aktionsplans „Eine erweiterte EU-Strategie für maritime Sicherheit angesichts sich wandelnder maritimer Bedrohungen“ vom 10. März 2023,
- die Schlussfolgerungen des Rates zu der überarbeiteten Strategie der EU für maritime Sicherheit (EUMSS) und dem dazugehörigen Aktionsplan vom 24. Oktober 2023,
- den Letta-Bericht „Much more than a market – Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens“ (Weit mehr als ein Markt – Geschwindigkeit, Sicherheit, Solidarität: Stärkung des Binnenmarkts zur Schaffung einer nachhaltigen Zukunft und von Wohlstand für alle Bürgerinnen und Bürger der EU) vom 17. April 2024,
- den Draghi-Bericht über die Zukunft der europäischen Wettbewerbsfähigkeit vom 9. September 2024,
- den Niinistö-Bericht „Safer together – Strengthening Europe’s Civilian and Military Preparedness and Readiness (Gemeinsam sicherer – Stärkung der zivilen und militärischen Vorsorge und Einsatzbereitschaft Europas) vom 30. Oktober 2024,
- den Bericht der Gruppe für Frequenzpolitik mit dem Titel „6G Strategic vision“ (Strategische 6G-Vision) vom 12. Februar 2025,
- die Gemeinsame Mitteilung an das Europäische Parlament und den Rat „EU-Aktionsplan für Kabelsicherheit“ vom 21. Februar 2025,

AUFBAUEND AUF

– dem Weißbuch der Kommission mit dem Titel „Wie kann der Bedarf an digitaler Infrastruktur in Europa gedeckt werden?“ vom 21. Februar 2024,
– der Empfehlung der Kommission vom 26. Februar 2024 über sichere und resiliente Seekabelinfrastrukturen,
– den Schlussfolgerungen des Rates vom 21. Mai 2024 zur Zukunft der Digitalpolitik der EU,
– den Schlussfolgerungen des Rates vom 6. Dezember 2024 zum Weißbuch der Kommission „Wie kann der Bedarf an digitaler Infrastruktur in Europa gedeckt werden?“ —

Allgemeiner Rahmen

1. STELLT FEST, dass die Konnektivitätsinfrastruktur der EU vor neuen und beispiellosen Herausforderungen steht, die sich aus einer zunehmend komplexen geopolitischen Lage – verdeutlicht durch die Auswirkungen des Angriffskriegs Russlands gegen die Ukraine – sowie aus der wachsenden Zahl physischer, Cyber- und hybrider Angriffe und Naturkatastrophen aufgrund des globalen Klimawandels ergeben; BETONT, dass Bedrohungen der Konnektivitätsinfrastruktur weitreichende geopolitische Auswirkungen auf die Außenpolitik der EU sowie auf das allgemeine Sicherheitsumfeld der EU haben;

2. ERKENNT AN, dass dieser Druck die Anfälligkeiten terrestrischer und nicht-terrestrischer Netze sowie von Seekabeln offenbart und daher – angesichts der kritischen Abhängigkeit unserer Gesellschaft und Wirtschaft von elektronischer Kommunikation und digitaler Infrastruktur – eine Neudefinition des strategischen Ansatzes der EU für die Entwicklung von Kommunikationsnetzen erfordert, um die digitale Souveränität und den wirtschaftlichen Wohlstand der EU auf offene Weise zu schützen, wobei besonderes Augenmerk auf die technologische Führungsrolle und die wirtschaftliche Widerstandsfähigkeit gelegt werden muss;

3. BETONT, dass ein umfassender Ansatz für die Entwicklung einer zuverlässigen und widerstandsfähigen Netzinfrastruktur von entscheidender Bedeutung ist, um neuen Herausforderungen im Zusammenhang mit häufigeren Naturkatastrophen, schädlichen Vorfällen, Cyberangriffen und geopolitischen Bedrohungen zu begegnen. Dieser Ansatz sollte berücksichtigt und in die mögliche Überarbeitung des bestehenden Rechtsrahmens einbezogen werden, unbeschadet der alleinigen Zuständigkeit der Mitgliedstaaten für die nationale Sicherheit;

4. ERKENNT AN, dass die überwiegende Mehrheit des interkontinentalen Datenverkehrs und Teile des innereuropäischen Datenverkehrs über Seekabelinfrastrukturen abgewickelt werden, die ein kritisches Backbone-Netz bilden, das zunehmend gefährdet ist, wie verschiedene Vorfälle insbesondere in der Ostsee zeigen; BEGRÜßT in diesem Zusammenhang die in der Empfehlung der Kommission über sichere und resiliente Seekabelinfrastrukturen enthaltenen Maßnahmen und TEILT DIE AUFFASSUNG, dass ein höheres Maß an Resilienz und technischer Integration sämtlicher Kommunikationskanäle – terrestrischer, nicht-terrestrischer und vor allem unterseeischer – als Voraussetzung für eine zuverlässige, resiliente und sichere Kommunikation wichtig ist, wie im Weißbuch der Kommission „Wie kann der Bedarf an digitaler Infrastruktur in Europa gedeckt werden?“ dargelegt;

5. NIMMT die Vision des Netzes für „Connected Collaborative Computing“ (im Folgenden „3C-Netz“) ZUR KENNTNIS, die im oben genannten Weißbuch der Kommission dargelegt wurde und von strategischer Bedeutung ist, um die digitale Souveränität der EU auf offene Weise zu schützen und voranzubringen, und die europäische Innovationen fördern und gleichzeitig ein Ökosystem für Konnektivität und Datenverarbeitungskapazitäten zur Unterstützung von daten- und KI-gestützten Anwendungen stärken kann;

6. WEIST DARAUF HIN, dass eine zuverlässige und resiliente Konnektivität durch technische Integration verschiedener Netzarten und Diversifizierung zu einer der wichtigsten Prioritäten geworden ist und vielschichtige, interoperable und redundante Netze erfordert; STELLT FEST, dass Kommunikationsstörungen abgemildert werden müssen, indem die physische und geografische Redundanz der Netzwerke sowie der Stromversorgung für die Konnektivitätsinfrastruktur für alle Backbone-Netze verbessert wird; ERKENNT AN, wie wichtig die Diversifizierung der Infrastruktur ist, insbesondere im Hinblick auf Notsituationen;

7. FORDERT die Festlegung eines strategischen Ansatzes für eine zuverlässige und resiliente Konnektivität, bei dem aktuelle und neu entstehende Technologien, insbesondere KI, 6G und Quantenkommunikation, berücksichtigt werden und der Schwerpunkt auf der Konvergenz verschiedener Netzelemente wie Fest-, Mobilfunk- und Satellitennetze (und anderer nicht-terrestrischer Elemente) zu einem kohärenten europäischen digitalen Ökosystem und Markt für Unternehmen jeder Größe liegen sollte;

8. STELLT FEST, dass bei diesem strategischen Ansatz die Konvergenz der verschiedenen Netztypen – einschließlich terrestrischer, nicht-terrestrischer und unterseeischer Kabel – berücksichtigt werden sollte, wobei unterschiedliche Geschäftsmodelle und aktuelle Trends berücksichtigt werden sollten, um so eine flächendeckende Konnektivität in ganz Europa zu fördern, die Wettbewerbsfähigkeit zu steigern und den europäischen Binnenmarkt zu stärken;

9. BETONT, dass die Konvergenz der verschiedenen Netztypen, die einen Zugang ermöglichen, eine Chance bietet, die Stärken der verschiedenen Technologien zu nutzen und ihre besten Merkmale zu kombinieren, dass aber auch die Bewältigung der Herausforderungen im Bereich der Cybersicherheit ein zentraler Schwerpunkt bleiben sollte;

10. FORDERT eine Koordinierung mit laufenden Forschungs- und Pilotinitiativen im Bereich Konnektivität, wie dem Gemeinsamen Unternehmen für intelligente Netze und Dienste, sowie mit anderen einschlägigen Konnektivitätsinfrastrukturprojekten, die aus EU-Mitteln wie Horizont Europa, Digitales Europa und der Fazilität „Connecting Europe“ unterstützt werden, einschließlich Seekabeln, Backbone-Konnektivitätsinfrastrukturen, Wiederherstellungs- und Sanierungskapazitäten durch die Nutzung bestehender Verlegeschiffskapazitäten und deren Verbesserung sowie Großpilotprojekte für 3C-Netzprojekte; BETONT, wie wichtig mögliche Finanzierungsprogramme sind, die zu den strategischen Prioritäten der Union beitragen könnten;

11. ERKENNT AN, dass die internationale Zusammenarbeit von entscheidender Bedeutung ist, wenn es darum geht, die Resilienz und Zuverlässigkeit der digitalen Infrastruktur weltweit zu verbessern und gleichzeitig einen menschenzentrierten und menschenrechtsbasierten Multi-Stakeholder-Ansatz für den digitalen Wandel zu fördern; BETONT, dass EU-Bewerberländer und andere Partnerländer durch die bestehenden Plattformen und EU-Initiativen wie Global Gateway und in den einschlägigen internationalen Foren wie der ITU unterstützt werden müssen, indem unter anderem technische Hilfe, Kapazitätsaufbau und finanzielle Unterstützung bereitgestellt werden, während gleichzeitig mit Partnerländern zusammengearbeitet werden muss, um Konvergenz bei politischen Ansätzen und regulatorischen und normativen Beispielen zu suchen und europäische Lösungen zu fördern;

Resilienz nach Netztypdiversifizierung und Interoperabilität

12. BETONT, dass eine zuverlässige und resiliente Konnektivität durch eine Diversifizierung der Netztypen verbessert werden kann, indem auf vielschichtige, interoperable terrestrische und nicht-terrestrische Kommunikationsmittel zurückgegriffen wird, die durch eine solide Backbone-Infrastruktur unterstützt werden, sowie Risikobewertungen und bewährte Verfahren für Abhilfemaßnahmen im Einklang mit der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2) und der Richtlinie über die Resilienz kritischer Einrichtungen;

13. ERKENNT AN, dass die rasche Entwicklung von Satellitenkommunikationssystemen, einschließlich Multikonstellationsnetze, von denen viele von Nicht-EU-Akteuren betrieben und entwickelt werden, Druck auf den Zugang zu Erdumlaufbahnen und Frequenzen ausübt; ERKENNT gleichzeitig die komplementäre Rolle von Satellitenkommunikationssystemen und anderen nicht-terrestrischen Kapazitäten für die ununterbrochene Verfügbarkeit von Kommunikationsdiensten, insbesondere in entlegenen und unterversorgten Regionen, AN, die kritische Redundanz und Resilienz gegen Störungen auf dem Boden bieten, was für die Bereitstellung von Sicherheits- und Katastrophenhilfediensten unter allen Umständen von besonderer Bedeutung ist;

14. BETONT die strategische Bedeutung von IRIS^2 – in die EURO QCI integriert wird – für die Bewältigung langfristiger Herausforderungen im Bereich der Sicherheit, des Schutzes und der Resilienz der Satellitenkommunikation; HEBT HERVOR, dass IRIS^2 eine wichtige Rolle dabei spielt, die bestehende technologische und industrielle Basis der europäischen Satellitenkommunikation zu untermauern, die Konnektivitätslücken in der gesamten Union zu schließen und die Unabhängigkeit der EU von außereuropäischen Anbietern von Kommunikationsdiensten – insbesondere von sicheren Kommunikationsdiensten – zu verbessern und zur Stärkung der digitalen Souveränität der Union auf offene Weise beizutragen; BETONT daher die Notwendigkeit einer zeitnahen Einführung von IRIS^2, die im Einklang mit internationalen und nationalen Rechtsrahmen die GOVSATCOM-Komponente des Weltraumprogramms ergänzt und integriert, um resiliente Kommunikationsdienste für staatliche und gewerbliche Nutzer bereitzustellen;

15. BETONT, wie wichtig es ist, für einen ausreichenden, sicheren, zuverlässigen, resilienten und geschützten Zugang zu geostationären, mittleren und niedrigen Erdumlaufbahnen und zu Funkfrequenzkapazitäten zu sorgen, die auf der Anwendung der in der ITU-Vollzugsordnung für den Funkdienst festgelegten Vorschriften beruhen; HEBT HERVOR, dass zur Gewährleistung gleicher Wettbewerbsbedingungen für alle Betreiber die Festlegung möglicher gemeinsamer Anforderungen für Satellitenkonstellationen, die Zugang zu nationalen und EU-Märkten erhalten, einschließlich solcher, die in Regulierungsrahmen außerhalb der EU registriert sind, auf den Ergebnissen der laufenden Beratungen in der Gruppe für Frequenzpolitik beruhen sollte; WÜRDIGT die laufenden Entwicklungen hin zu konvergierenden Mobilfunk- und Satellitentechnologien, einschließlich der jüngsten 5G-Normung und der Entwicklung des 6G-Netzes, die eine nahtlose Verfügbarkeit elektronischer Kommunikationsdienste unabhängig vom Standort gewährleisten und gleichzeitig die Entwicklung europäischer Innovationskapazitäten und den Wettbewerb in der EU zum Vorteil der Endnutzer unterstützen;

16. ERKENNT FERNER das Transformationspotenzial ergänzender Direct-to-Device-Satellitendienste (D2D) AN, die über Smartphone-Anwendungen für Verbraucher hinausgehen und auf mobilitätsbezogene vertikale Märkte wie den Verkehrs-, den Luftfahrt- und den maritimen Sektor ausgerichtet sind; WEIST auf die entscheidende Rolle HIN, die D2D-Dienste bei der Verbesserung öffentlicher Dienste, unter anderem des Katastrophenschutzes, mit weitreichenden Vorteilen auf zahlreichen Gebieten spielen können; ERKENNT AN, dass die weitere Konvergenz von Satelliten- und Mobilfunktechnologien das Potenzial hat, das sozioökonomische Wachstum zu steigern, die Resilienz der Netze zu verbessern, die digitale Kluft zu überbrücken und globale Herausforderungen im Bereich der Konnektivität zu bewältigen; FORDERT die frühzeitige Integration von D2D-Diensten in das globale Kommunikationssystem von IRIS^2, um die Wettbewerbsfähigkeit der EU zu stärken;

17. HEBT die wachsende Herausforderung durch absichtliches Stören (Jamming) und Spoofing globaler Satellitennavigationssysteme (GNSS) HERVOR, die sich auf eine Vielzahl kritischer Infrastrukturen und Dienste auswirken; WÜRDIGT die Arbeit der EU-Taskforce zu GNSS-Störungen; RUFT zu koordinierten Bemühungen der EU AUF, einen robusten Mechanismus für die Verwaltung von Informationen im Zusammenhang mit GNSS-Störungen einzurichten, um die zügige Berichterstattung, den Datenaustausch im Rahmen der nationalen Sicherheitsanforderungen und der Zuständigkeiten der Mitgliedstaaten sowie koordinierte Reaktionsmaßnahmen in allen Mitgliedstaaten zu gewährleisten; UNTERSTREICHT, dass eine präzise Zeitsynchronisierung durch GNSS für viele kritische Einrichtungen und strategische Wirtschaftszweige, darunter die Luftfahrtindustrie, die Finanz- und die elektronische Kommunikationsbranche sowie der Energie-, der Verkehrs- und der Handelssektor, von wesentlicher Bedeutung ist und dass daher jede Störung dieser Systeme weitreichende wirtschaftliche und gesellschaftliche Folgen haben kann; FORDERT Maßnahmen zur Bereitstellung alternativer Lösungen, um den fortwährenden Betrieb der GNSS zu gewährleisten;

18. STELLT FEST, dass Investitionen in nachhaltige Technologien wie die Versorgung mit Energie aus erneuerbaren Quellen, die Energiespeicherung und intelligente Messsysteme nicht nur zur Verringerung des CO_2-Fußabdrucks beitragen, sondern auch zur Stärkung der Resilienz der Konnektivitätsinfrastruktur und zur Gewährleistung des ununterbrochenen Zugangs zu einer Energiequelle in Notlagen;

19. FORDERT die Mobilisierung strategischer Investitionen zur Verbesserung des Schutzes und der Resilienz der digitalen Infrastruktur, mit besonderem Schwerpunkt auf wichtigen Kabelverbindungen für Backbone-Netze, zum Schutz grundlegender strategischer Interessen der EU im Atlantik, in der Ostsee, im Schwarzen Meer, im Mittelmeer, in der Nordsee, in der Arktis sowie in Gebieten in äußerster Randlage; BETONT die dringende Notwendigkeit einer umfassenden Unterstützung der Seekabelinfrastruktur, wie sie im EU-Aktionsplan für Kabelsicherheit hervorgehoben wurde, einschließlich der Prävention von Bedrohungen, der Risikoerkennung, der raschen Reaktion auf Vorfälle, der Abschreckung sowie der Wiederherstellungs- und Sanierungskapazitäten durch die Nutzung bestehender Verlegeschiffskapazitäten – einschließlich deren Verbesserung – auf der Grundlage der Arbeit der informellen Expertengruppe für Seekabelinfrastruktur in Abstimmung mit der Gruppe für die Resilienz kritischer Einrichtungen (CER) und der NIS-Kooperationsgruppe; UNTERSTREICHT die Bedeutung des Ausbaus von Kapazitäten zur Erholung nach unbeabsichtigten Vorfällen oder Sabotageakten; BETONT, dass die Redundanz der grenzüberschreitenden terrestrischen Glasfaserverbindungen und der Seekabelinfrastrukturen innerhalb Europas für die globale Konnektivität sichergestellt werden muss; HEBT HERVOR, dass für die Umsetzung der Maßnahmen des EU-Aktionsplans eine enge Zusammenarbeit mit den Mitgliedstaaten im Einklang mit den geltenden Vorschriften erforderlich ist;

20. WÜRDIGT laufende Initiativen zur Resilienzförderung, etwa im Rahmen der Empfehlung 2023/C 20/01 des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur und des Berichts der NIS-Kooperationsgruppe zur Cybersicherheit und Resilienz der Kommunikationsinfrastrukturen und -netze Europas als Folgemaßnahme zum Aufruf von Nevers vom 9. März 2022;

21. UNTERSTREICHT die entscheidende Bedeutung der Cybersicherheit für die Entwicklung einer zuverlässigen und resilienten Konnektivitätsinfrastruktur sowie für die Schaffung von Sicherheit zur Verringerung der Risiken von wechselseitigen Abhängigkeiten in Technologie und Handel; STELLT FEST, wie wichtig Risikobewertungen für die Verringerung von Sicherheitsrisiken und Abhängigkeiten sowie die Nutzung vertrauenswürdiger Anbieter beim Aufbau von Kommunikationsnetzen sind; UNTERSTREICHT, wie wichtig es ist, die NIS-2-Richtlinie und die CER-Richtlinie umzusetzen, um die Sicherheit der digitalen Infrastrukturen und der wesentlichen Dienste zu gewährleisten; HEBT HERVOR, dass die Risiken im Zusammenhang mit der Lieferkettensicherheit für alle Arten von Netzen und Informationssystemen gemindert werden müssen und dass zügig ein Instrumentarium von Maßnahmen zur Verringerung von Risiken in kritischen IKT-Lieferketten angenommen werden muss; RUFT in diesem Zusammenhang dazu AUF, die vollständige Umsetzung des Instrumentariums für die 5G-Cybersicherheit sowie der Maßnahmen zur Lieferkettensicherheit im Einklang mit der NIS-2-Richtlinie und der CER-Richtlinie zu beschleunigen, insbesondere die koordinierte Bewertung der Sicherheitsrisiken der genannten kritischen Lieferketten auf Unionsebene, und BEFÜRWORTET Beratungen über einen stärker harmonisierten Ansatz zur Bewältigung neu auftretender Cyberbedrohungen in der elektronischen Kommunikation;

22. STELLT FEST, dass es von strategischer Bedeutung ist, europäische, technisch integrierte und resiliente Kommunikationsnetze zu entwickeln, die eine flächendeckende Versorgung gewährleisten und durch Diversifizierung und Redundanz der Netztypen die Resilienz ihrer verschiedenen Elemente maximieren; BETONT, dass die Entwicklung solcher Netze den Besonderheiten der Mitgliedstaaten Rechnung tragen und von der Marktdynamik angetrieben werden sollte, und zwar in Verbindung mit einer gezielten Unterstützung durch die EU, unter anderem durch Leitlinien und Finanzierungsmittel für strategische Konnektivitätsprojekte;

Binnenmarkt für zuverlässige und resiliente Konnektivität

23. ERKENNT AN, dass eine zuverlässige und resiliente Konnektivitätsinfrastruktur das Rückgrat und ein grundlegender Baustein des Binnenmarkts ist, der eine wichtige Triebkraft für Wettbewerbsfähigkeit und Innovation in der EU darstellt, wodurch die Union in der digitalen Wirtschaft eine weltweit führende Stellung erlangen und ihre digitale Souveränität auf offene Weise stärken konnte;

24. UNTERSTREICHT, dass der Binnenmarkt für elektronische Kommunikation gegebenenfalls durch Maßnahmen zur weiteren Harmonisierung und durch die Verbesserung der grenzüberschreitenden Konnektivität vertieft werden sollte, wobei die unterschiedlichen Geschäftsmodelle der Dienstleister, regionale Gegebenheiten und die nationale Zuständigkeit der Mitgliedstaaten bei der Anwendung harmonisierter Vorschriften berücksichtigt werden sollten; BETONT, dass die Verbesserungen des Binnenmarkts für elektronische Kommunikation die Wettbewerbsfähigkeit und die digitale Souveränität der Union auf offene Weise stärken und zu einer flächendeckenden Versorgung durch zuverlässige und resiliente Netze beitragen werden, und dies zum Vorteil der Bürger und Unternehmen der EU;

25. STELLT FEST, dass die Förderung technisch integrierter und resilienter europäischer Kommunikationsnetze neue Marktchancen im Bereich der elektronischen Kommunikation sowie horizontal in der digitalen Wirtschaft eröffnen kann, wodurch die globale Wettbewerbsfähigkeit der Union durch die Begünstigung technologischer Innovationen gestärkt wird;

26. UNTERSTREICHT, dass Funkfrequenzen eine Schlüsselrolle zum Vorteil des Binnenmarkts, der EU-Wirtschaft und der Gesellschaft insgesamt spielen; HEBT HERVOR, dass die effiziente und koordinierte Nutzung von Funkfrequenzen die Politik der EU unterstützt und gleichzeitig den gesellschaftlichen Nutzen maximiert und dazu beiträgt, das Ziel der Verbesserung des Binnenmarkts zu erreichen; BEFÜRWORTET die Bewertung des Frequenzbedarfs, einschließlich der für den 6G-Ausbau geeigneten Frequenzbänder, auf der Grundlage der Anforderungen an die Versorgung und Kapazität für Nutzungsfälle terrestrischer und nicht-terrestrischer Netze;

27. WÜRDIGT das erfolgreiche europäische Modell der schrittweisen Frequenzharmonisierung und die Rolle der ITU bei der Frequenzverwaltung; FORDERT die Kommission AUF, den Unterstützungsmechanismus auf EU-Ebene für die Mitgliedstaaten zu verbessern, um einen konstruktiven Rahmen zu schaffen, der es den Mitgliedstaaten ermöglicht, auf grenzüberschreitende funktechnische Störungen innerhalb der EU und mit Drittländern zu reagieren, und nicht auf rein technische Fragen beschränkt ist;

28. BEFÜRWORTET die Einführung und Weiterentwicklung zukunftsfähiger, sicherer und vertrauenswürdiger Standards als Basis für technologische Entwicklungen zur Aufrechterhaltung der digitalen Souveränität der EU auf offene Weise und zur Förderung von Innovation und Zusammenhalt in der elektronischen Kommunikationsbranche der EU; ERSUCHT die Europäische Kommission, den Europäischen Auswärtigen Dienst und die Mitgliedstaaten, den „Team Europa"-Ansatz in internationalen Foren zu verstärken, indem sie sich aktiv an globalen Normungsprozessen beteiligen, Standards fördern, die in Europa auf der Basis von EU-Grundwerten wie den Menschenrechten entwickelt wurden, und für eine koordinierte europäische Strategie für digitale Infrastruktur sorgen, die alle Kommunikationsebenen umfasst;

29. FORDERT ein höheres Maß an Resilienz durch Diversifizierung und eine nahtlose, flächendeckende Konnektivität durch die Weiterentwicklung technisch integrierter und resilienter europäischer Kommunikationsnetze im Rahmen eines mehrstufigen Ansatzes, der unter anderem Folgendes umfasst: Normungstätigkeiten, gezielte potenzielle Finanzinstrumente zur Unterstützung der Entwicklung solcher Netze sowie Leitlinien zur Erleichterung ihrer marktorientierten Einführung.

30. ERSUCHT die Kommission, dem Rat über wichtige Entwicklungen in Bezug auf technisch integrierte und resiliente europäische Kommunikationsnetze Bericht zu erstatten. Dies sollte zum Informationsaustausch und zur Verfolgung der Fortschritte bei der Verwirklichung einer nahtlosen und flächendeckenden Konnektivität beitragen;

31. ERSUCHT die Kommission, auf der Arbeit der informellen Expertengruppe für die Seekabelinfrastruktur im Rahmen des strategischen politischen Ansatzes aufzubauen, der in der Empfehlung über sichere und resiliente Seekabelinfrastrukturen sowie im EU-Aktionsplan für Kabelsicherheit festgelegt ist, und auf der Grundlage der Ergebnisse der Gruppe für die Resilienz kritischer Einrichtungen (CER), der NIS-Kooperationsgruppe und der informellen Expertengruppe für Seekabelinfrastruktur konkrete Vorschläge zur weiteren Förderung der Zuverlässigkeit und Resilienz dieser Infrastrukturen als wesentlicher Bestandteil der europäischen Kommunikationsnetze zu prüfen, wobei darauf hinzuweisen ist, dass die nationale Sicherheit in die alleinige Zuständigkeit der Mitgliedstaaten fällt;

32. STELLT FEST, dass eine fortwährende und ununterbrochene Konnektivität für eine sichere und ordnungsgemäß funktionierende Union von wesentlicher Bedeutung ist; IST SICH der sich häufenden Naturkatastrophen und anderer Bedrohungen BEWUSST, die die Redundanz der Stromversorgung für die Netze zu einer dringenden Herausforderung machen; FORDERT die Kommission AUF, geeignete Maßnahmen, auch in Form finanzieller Unterstützung, zu analysieren und vorzuschlagen, ohne den Verhandlungen über den nächsten mehrjährigen Finanzrahmen vorzugreifen;

33. FORDERT die Kommission AUF, die Möglichkeit einer koordinierten Initiative zur Planung und Entwicklung eines zuverlässigen und resilienten Netzes digitaler Infrastrukturen und Kapazitäten zu prüfen, das terrestrische, unterseeische und satellitengestützte Backbone-Netze in der gesamten Union und mit internationalen Partnerländern umfasst, beispielsweise durch die Nutzung des Rahmenprogramms für die transeuropäischen Netze und die Schaffung eines TEN-D-Instruments (Transeuropäische Netze – Digital); BEGRÜßT den Ansatz der Kommission für die Arktis-Konnektivitätsinitiative sowie die laufenden Bemühungen zur Stärkung der Resilienz der digitalen Infrastruktur der Küstenregionen der EU; HEBT HERVOR, dass bei der Bewertung von Kabelvorhaben von europäischem Interesse (CPEI) unter Berücksichtigung der Empfehlung (EU) 2024/779 klare, integrierte und greifbare Kriterien festgelegt und befolgt werden müssen, um Sicherheit und Resilienz zu verbessern und internationale Partnerschaften zu fördern;

34. VERPFLICHTET SICH, den strategischen Ansatz der EU für die Kommunikationsinfrastruktur kontinuierlich zu überwachen und anzupassen, um neue technologische, geopolitische und ökologische Herausforderungen zu bewältigen und eine zuverlässige und resiliente Konnektivität in der gesamten Union zu gewährleisten.