Council of the European Union

Brussels, 6 June 2025
(OR. en)

9953/25

TELECOM 180
CYBER 160
COMPET 496
MI 361
PROCIV 66

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7929/25
Subject:	Conclusions on reliable and resilient connectivity - Council Conclusions (6 June 2025)

Delegations will find in the annex the Council Conclusions on reliable and resilient connectivity as approved by the Transport, Telecommunications and Energy Council at its meeting held on 6 June 2025.

ANNEX

Council Conclusions on reliable and resilient connectivity

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING:

- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 on establishing the European Electronic Communications Code,
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive),
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC,
- The Joint Communication to the European Parliament and the Council on the update of the EU Maritime Security Strategy and its Action Plan "An enhanced EU Maritime Security Strategy for evolving maritime threats" of 10 March 2023,
- The Council Conclusions of 24 October 2023 on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan,
- The Letta Report “Much more than a market – Speed, Security, Solidarity. Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens” of 17 April 2024,
- The Draghi Report “The future of European competitiveness” of 9 September 2024,
- The Niinistö Report “Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness” of 30 October 2024,
- The Radio Spectrum Policy Group Report “6G Strategic vision” of 12 February 2025,
- The Joint Communication to the European Parliament and the Council “EU Action Plan on Cable Security” of 21 February 2025,

BUILDING ON:

- The Commission White Paper on “How to master Europe’s digital infrastructure needs?” of 21 February 2024,
- The Commission Recommendation of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures,
- The Council Conclusions of 21 May 2024 on “The Future of EU Digital Policy”,
- The Council Conclusions of 6 December 2024 on the Commission White Paper “How to master Europe’s digital infrastructure needs?”,

General framework

1. NOTES that the EU's connectivity infrastructure faces new and unprecedented challenges arising from an increasingly complex geopolitical situation, as underscored by the impact of Russia's war of aggression against Ukraine, as well as from the growing number of physical, cyber and hybrid attacks and occurrences of natural disasters due to global climate change. EMPHASISES that threats to connectivity infrastructure have far reaching geopolitical implications on the EU's foreign policy as well as on the overall security environment of the EU.

2. ACKNOWLEDGES that these pressures expose the vulnerabilities of terrestrial and non-terrestrial networks, and of submarine cables, thus requiring a redefinition of the EU's strategic approach to the communications network development in light of the critical dependence of our society and economy on electronic communications and digital infrastructure, to safeguard the EU's digital sovereignty and economic prosperity in an open manner, with particular attention to technological leadership and economic resilience.

3. STRESSES that a comprehensive approach to the development of a reliable and resilient network infrastructure is essential for addressing new challenges related to more frequent natural disasters, damaging incidents, cyber-attacks and geopolitical related threats. This approach should be taken into account and integrated into the possible revision of the existing legal framework without prejudice to Member States' sole responsibility for national security.

4. RECOGNISES that the large majority of intercontinental and parts of intra-European internet traffic runs over submarine cable infrastructures, which form a critical backbone network, being increasingly at risk, as demonstrated by various incidents notably in the Baltic Sea. WELCOMES in this regard the measures in the Commission Recommendation on "Secure and Resilient Submarine Cable Infrastructures" and AGREES on the importance of a higher level of resilience and technical integration of all communication channels - terrestrial, non-terrestrial and, importantly, submarine - as a precondition for reliable, resilient and secure communications, as stated in the Commission's White Paper on "How to master Europe's digital infrastructure needs?".

5. NOTES the vision of the Connected Collaborative Computing Network ("3C Network") set out in the Commission White Paper mentioned above, which is of strategic importance to safeguard and advance the EU's digital sovereignty in an open manner and can enhance European innovations whilst strengthening an ecosystem of connectivity and computational capacity in support of data and AI-based applications.

6. RECALLS that reliable and resilient connectivity through technical integration of different network types and diversification has emerged as one of the key priorities, requiring multi-layered, interoperable and redundant networks. NOTES the need to mitigate communication disruptions by improving the physical and geographic redundancy of networks as well as of the power supply for connectivity infrastructure for all the backbone networks. RECOGNIZES the importance of diversification of infrastructure, in particular in emergency situations.

7. CALLS FOR the establishment of a strategic approach for reliable and resilient connectivity that takes into account current and emerging technologies, especially AI, 6G and quantum communications, with a focus on the convergence of diverse network elements such as fixed, mobile and satellite (and other non-terrestrial elements) into a cohesive European digital ecosystem and market for companies of all sizes.

8. NOTES that this strategic approach should take into account the convergence of different network types - including terrestrial, non-terrestrial, and submarine cables - while considering diverse business models and current trends, thus fostering ubiquitous and seamless connectivity across Europe, enhancing competitiveness and reinforcing the European Single Market.

9. EMPHASISES that the convergence of different network types providing access presents an opportunity to take advantage of the strengths of different technologies and combine the best of their characteristics, but addressing cybersecurity challenges should also remain a key focus.

10. CALLS FOR coordination with ongoing research and piloting initiatives on connectivity, such as the Smart Networks and Services Joint Undertaking, as well as other relevant connectivity infrastructure projects supported by EU funds like Horizon Europe, Digital Europe and the Connecting Europe Facility (CEF2 Digital), including submarine cables, backbone connectivity infrastructures, recovery and repair capacities through leveraging existing cable vessel capacities, and improving them, as well as large scale pilots for 3C Network projects. STRESSES the importance of possible funding programmes that could contribute to the Union's strategic priorities.

11. RECOGNISES the critical importance of international cooperation in enhancing global digital infrastructure resilience and reliability while promoting a multi-stakeholder, human-centric and human rights-based approach to digital transformation. HIGHLIGHTS the need for supporting EU candidate countries and other partner countries through the existing platforms and EU initiatives, like Global Gateway, and within the relevant international fora such as the ITU, providing inter alia technical assistance, capacity-building and financial support, while collaborating with partner countries to search convergence on policy approaches and regulatory and normative examples, and promote European solutions.

Resilience by network type diversification and interoperability

12. EMPHASISES that reliable and resilient connectivity can be improved through network type diversification by relying on multi-layered, interoperable terrestrial and non-terrestrial communication means supported by a robust backbone infrastructure, as well as risk assessments and good practices on mitigating measures in line with the Directive on measures for a high common level of cybersecurity across the Union (NIS2) and the Critical Entities Resistance (CER) Directive.

13. ACKNOWLEDGES that the rapid development of satellite communication systems, including multi-constellation networks, a large number of which are operated and developed by non-EU actors, puts pressure on access to Earth's orbits and spectrum. RECOGNISES at the same time the complementary roles of satellite communication systems and other non-terrestrial capabilities, for uninterrupted availability of communication service, in particular to remote and underserved regions, providing critical redundancy and resilience against ground-based disruptions, which are particularly important for the provision of safety and disaster relief services in all circumstances.

14. EMPHASISES the strategic importance of IRIS² - which will integrate EURO QCI - for addressing long-term challenges in satellite communications security, safety, and resilience. Stresses the role of IRIS² in underpinning the existing European satellite communication technological and industrial base, bridging the connectivity gaps across the Union and improving the EU's independence from non-European providers for communication services - particularly secure ones, and contributing to the reinforcement of the Union's digital sovereignty in an open manner. EMPHASISES therefore the need for a timely rollout of IRIS², complementing and integrating the GOVSATCOM space programme component, consistent with international and national regulatory frameworks to provide resilient communication services for governmental users and commercial users.

15. EMPHASISES the importance of ensuring sufficient, safe, reliable, resilient and secure access to geostationary, medium and low earth orbits and to radio spectrum capacity which rely on the application of rules defined in the ITU Radio Regulations. STRESSES that, in order to guarantee a level playing field for all operators, the establishment of possible common requirements for satellite constellations accessing national and EU markets, including those registered under regulatory frameworks outside of the EU, should be based on the outcome of the ongoing discussion within the Radio Spectrum Policy Group (RSPG). ACKNOWLEDGES the ongoing evolution towards converging mobile and satellite technologies including the recent 5G standardisation and 6G development, which ensures seamless availability of electronic communication services regardless of the location, while supporting the development of European innovation capabilities and competition in the EU for the benefit of end users.

16. FURTHER RECOGNISES the transformative potential of complementary Direct-to-Device (D2D) satellite services, which extend beyond consumer smartphone applications, to address mobility-related vertical markets such as transport, aeronautical, and maritime sectors. NOTES the critical role that D2D services can play in improving public services, including civil protection, with far-reaching benefits across multiple domains. ACKNOWLEDGES that further convergence of satellite and mobile technologies has the potential to drive socio-economic growth, improve network resilience, bridge the digital divides and address global connectivity challenges. CALLS for the early integration of D2D services into the IRIS² global communication system in order to reinforce the EU's competitiveness.

17. HIGHLIGHTS the growing challenge coming from the deliberate jamming and spoofing of Global Navigation Satellite Systems (GNSS) that impact a wide range of critical infrastructure and services. ACKNOWLEDGES the work of the EU GNSS Interference Task Force. CALLS FOR a coordinated EU effort to establish a robust mechanism for managing information related to GNSS disruptions, ensuring timely reporting, data sharing within the limits of national security requirements and Member States' competences, as well as coordinated response measures across Member States. UNDERLINES that precise time synchronisation provided by GNSS is essential for many critical entities and strategic industries, including aviation, finance and electronic communications, as well as energy, transportation and commerce, and therefore any kind of disruption to these systems may have far-reaching economic and societal consequences. CALLS for actions to provide alternative solutions to the continuous functionality provided by GNSS.

18. NOTES that investments in sustainable technologies such as renewable energy supply, energy storage and smart metering contribute not only to the reduction of the carbon footprint but also to strengthening the resilience of connectivity infrastructure, ensuring uninterrupted access to a source of power at a time of emergency.

19. CALLS FOR the mobilisation of strategic investments to enhance digital infrastructure protection and resilience, with a particular focus on critical cables for backbone networks, to protect vital strategic interests of the EU in the Atlantic Ocean and the Baltic, Black, Mediterranean and North seas, the Arctic region, as well as in outermost regions. STRESSES the urgent need for comprehensive support for submarine cable infrastructure, as raised in the EU Action Plan on Cable Security, including threat prevention, risk detection, rapid incident response, deterrence, as well as recovery and repair capacities through leveraging existing cable vessel capacities, and improving them, based on the work of the Submarine Cable Infrastructure informal Expert Group, in coordination with the Critical Entities Resilience (CER) Group and NIS Cooperation Group. UNDERSCORES the importance of increased capabilities in order to recover from unintended incidents or sabotage. EMPHASISES the need to ensure redundancy of cross-border terrestrial fibre-optic connections and submarine cable infrastructures within Europe, for global connectivity. STRESSES the need to work in close cooperation with the Member States according to existing rules for the implementation of measures from the EU Action Plan.

20. RECOGNISES ongoing initiatives on fostering resilience such as in the framework of Council Recommendation 2023/C 20/01 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure and the NIS Cooperation Group Report on cybersecurity and resilience of Europe's communications infrastructures and networks as a follow-up to the Nevers Call of 9 March 2022.

21. UNDERSCORES the critical importance of cybersecurity in developing reliable and resilient connectivity infrastructure, as well as security reducing the risks of technological and trade interdependencies. RECOGNISES the importance of risk assessments to reduce security risks and dependencies, as well as using trusted suppliers when deploying communication networks. UNDERLINES the importance of transposing and implementing the NIS 2 and CER Directives to ensure that the digital infrastructures and essential services are secure. STRESSES the need to mitigate risks associated with supply chain security for all types of networks and information systems and the need for the rapid adoption of a toolbox of measures for reducing critical ICT supply chain risks. In this context, CALLS to accelerate the full implementation of the 5G cybersecurity toolbox, as well as the measures on supply chain security in line with the NIS 2 and CER Directives, in particular the Union level coordinated security risk assessment of the aforementioned critical supply chains and ENCOURAGES discussions about a more harmonised approach to address emerging cybersecurity threats in electronic communications.

22. RECOGNISES the strategic importance of developing European technically integrated resilient communication networks that ensure ubiquitous coverage and maximise resilience across their various elements through network type diversification and redundancy. EMPHASISES that the development of such networks should take into account Member States' specificities and be driven by market dynamics accompanied by targeted EU support, including through guidelines and funding for strategic connectivity projects.

Single market for reliable and resilient connectivity

23. ACKNOWLEDGES that reliable and resilient connectivity infrastructure constitutes the backbone and a fundamental building block of the Single Market, which is a main driver for EU competitiveness and innovation, positioning the Union as a global leader in the digital economy, strengthening its digital sovereignty in an open manner.

24. UNDERLINES that the Single Market for electronic communications should be deepened through further harmonisation where necessary, and improved cross-border connectivity, while recognising different business models of service providers, regional circumstances and the national competence of Member States in the application of harmonised rules. EMPHASISES that the improvements of the Single Market for electronic communications will reinforce the Union's competitiveness and digital sovereignty in an open manner, as well as contribute to ubiquitous coverage by reliable and resilient networks, for the benefit of EU citizens and businesses.

25. NOTES that fostering technically integrated and resilient European communication networks can open new market possibilities within the electronic communications sector, as well as horizontally in the digital economy, enhancing the Union’s global competitiveness by driving technological innovation.

26. UNDERSCORES that radio spectrum plays a key role for the benefit of the Single Market, the EU economy and society as a whole. STRESSES that the efficient and coordinated use of radio spectrum supports EU policies, while maximising societal value, and serves to reach the objective of the improvement of the Single Market. ENCOURAGES the assessment of spectrum needs, including bands as suitable candidates for 6G rollout, based on coverage and capacity requirements for terrestrial and non-terrestrial networks use cases.

27. ACKNOWLEDGES the successful European model of gradual spectrum harmonisation and the role of the ITU in radio spectrum management. CALLS on the Commission to enhance the EU-level support mechanism for the Member States which will provide a constructive framework that allows the Member States to respond to cross-border interferences cases within the EU and with third countries, not limited to purely technical issues.

28. ENCOURAGES the deployment and further development of futureproof, secure, and trustworthy standards as a baseline for technological developments, maintaining the EU's digital sovereignty in an open manner, and driving innovation and cohesion of the EU electronic communications sector. INVITES the European Commission, the European External Action Service and Member States to enhance the Team Europe approach in international fora by actively participating in global standard-setting processes, promoting European-developed standards based on core values shared by the EU such as human rights, and ensuring a coordinated European digital infrastructure strategy that includes all communication layers.

29. CALLS FOR a higher level of resilience by diversification and seamless, ubiquitous connectivity through further developing technically integrated and resilient European communication networks in a multilayered approach encompassing among others: standardisation activities, possible targeted financial instruments supporting the development of such networks, and guidelines facilitating market-driven deployment.

30. INVITES the Commission to report to the Council on significant developments regarding technically integrated and resilient European communication networks. This should contribute to exchanging information and monitoring progress in achieving seamless and ubiquitous connectivity.

31. INVITES the Commission to build on the work of the Submarine Cable Infrastructure informal Expert Group under the strategic policy approach laid out in the Recommendation on Secure and Resilient Submarine Cable Infrastructures as well as in the EU Action Plan on Cable Security, and reflect on concrete proposals to further promote the reliability and resilience of these infrastructures as a crucial part of European communication networks based on the work of the Critical Entities Resilience (CER) Group and NIS Cooperation Group, and the Submarine Cable Infrastructure informal Expert Group, whilst recalling that national security is the sole responsibility of Member States.

32. RECOGNISES that continuous and uninterrupted connectivity is essential for a secure and properly functioning Union. TAKES INTO CONSIDERATION the more frequent natural disasters and other threats, which make the redundancy of the supply of power for networks an urgent challenge. CALLS on the Commission to analyse and propose appropriate measures, including financial support without pre-empting the negotiations on the next Multiannual Financial Framework.

33. CALLS on the Commission to assess the possibility for a coordinated initiative for planning and developing a reliable and resilient network of digital infrastructures and capacities, encompassing backbone terrestrial, submarine and satellite networks, across the Union and with international partner countries, for example by using the Trans-European Networks framework and establishing a TEN-D (Trans-European Networks - Digital) instrument. WELCOMES the Commission's approach to the Arctic Connectivity Initiative as well as ongoing efforts to reinforce the resilience of the digital infrastructure of the EU's maritime regions. STRESSES the need to define and follow clear, integrated, and tangible criteria, taking into account Recommendation (EU) 2024/779, when assessing Cable Projects of European Interest (CPEIs), improving security and resilience and promoting international partnerships.

34. COMMITS to continuously monitor and adapt the EU's strategic approach to communication infrastructure to address emerging technological, geopolitical, and environmental challenges, ensuring reliable and resilient connectivity across the Union.