Council of the European Union

Brussels, 22 November 2019
(OR. en)

14368/19

LIMITE

TELECOM 366
CYBER 318
COMPET 761
MI 803
CONSOM 314

NOTE

From:	Permanent Representatives Committee (Part 1)
To:	Council
No. prev. doc.:	14147/19
Subject:	Conclusions on the significance of 5G to the European Economy and the need to mitigate the security risks linked to 5G - Adoption

1. On 22 October 2019 the Finnish Presidency presented its draft Council Conclusions on the significance of 5G to the European economy and the need to mitigate the security risks linked to 5G.

2. The Working Party on Telecommunications and Information Society discussed the document at its meetings on 22 October, 5, 14 and 18 November 2019 and has agreed on the draft Council Conclusions as set out in the Annex to this document.

3. The Permanent Representatives Committee discussed the draft Council Conclusions contained in the Annex on 22 November 2019 and has agreed to transmit it to the Council for adoption.

4. Once adopted by the Council, the Conclusions will be published in the Official Journal of the European Union.

ANNEX

Draft Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G

THE COUNCIL OF THE EUROPEAN UNION

Having regard to the potential of 5G networks for the European economy, the EU single market and European citizens

1. ACKNOWLEDGES that 5G is an evolution of 4G networks and that 5G will increase the potential of mobile networks service provision and at the same time enable innovative business models and public services across multiple sectors as well as other opportunities for European citizens, telecommunications operators, companies, including SMEs, the public sector as well as other stakeholders.

2. RECALLS that the Union has developed a legal framework for tackling and mitigating cybersecurity risks linked to 5G, such as the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (EECC) and Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

3. RECOGNIZES the need to meet the ambitious objectives of the 5G Action Plan adopted by the Commission in 2016 and the Tallinn Ministerial Declaration on 5G, as well as the related roadmap agreed among Member States in 2017 building on Gigabit Society goals.

4. STRESSES that 5G networks will form a part of crucial infrastructure for the operation and maintenance of vital societal and economic functions and a wide range of services essential for functioning of the internal market including its digital transformation and in this regard EMPHASISES the importance of European technological sovereignty and promoting globally the EU approach to cyber security of future electronic communication networks.

5. EMPHASISES the need to ensure the swift demand based roll-out of the 5G networks and that 5G is a key asset for European competitiveness, sustainability and a major enabler for future digital services as well as a priority for the European Single Market. In this context, the Council STRESSES also the importance of co-operation of the Member States in the take-up of 5G networks in cross-border areas between Member States.

6. RECOGNISES the need to raise public awareness about the possibilities of 5G and increase competences within developers and different user groups, and that the public sector has a role in encouraging the take up of 5G by leading by example, and encourages all relevant stakeholders to engage in the sharing of information and experience in support of the successful roll out of 5G, including questions related to the measurements of electromagnetic fields (EMF) limits.

7. ENCOURAGES the Commission and the Member States to take the necessary steps to make the EU a leading market for deployment of 5G networks and development of 5G-based solutions that foster growth and innovation, improve everyday life of citizens and businesses, enable new services and applications as well as bring more opportunities for the whole society in key sectors and industries such as energy, health care, agriculture, finance and mobility.

Having regard to the challenges of 5G networks

8. EMPHASISES the importance of safeguarding the security and resilience of electronic communications networks and services, in particular as regards 5G, following a risk-based approach.

9. STRESSES that while the deployment of 5G networks brings new opportunities, the profound changes that 5G technologies will bring to the networks, devices and applications, and the increased security concerns related to the integrity and availability of 5G networks, in addition to confidentiality and privacy, make it necessary for the EU and the Member States to pay particular attention to promoting the cybersecurity of these networks and all services depending on electronic communications.

10. WELCOMES the ongoing joint European efforts on safeguarding the security of 5G networks based in particular on the Commission Recommendation on Cyber Security of 5G Networks and STRESSES the importance of a coordinated approach and effective implementation of the Recommendation in order to avoid fragmentation in the Single Market.

11. WELCOMES the European coordinated risk assessment published on 9th October 2019 as a first deliverable following the Recommendation.

12. EMPHASISES that the technological changes introduced by 5G will increase the overall attack surface and require particular attention to the risk profiles of individual suppliers.

13. STRESSES that in addition to the technical risks related to cybersecurity of 5G networks, also non-technical factors such as the legal and policy framework to which suppliers may be subject to in third countries, should be considered.

14. REAFFIRMS the importance for the Member States to consider the need to diversify suppliers in order to avoid or limit the creation of a major dependency on a single supplier, as it increases the exposure to the consequences of a potential failure of this supplier.

15. HIGHLIGHTS the importance of assessing the risks related to interdependencies between 5G networks and other critical public and private systems and services.

THE COUNCIL THEREFORE

16. EMPHASISES that a swift and secure roll-out of the 5G networks is key for enhancing the competitiveness of the EU and requires a coordinated approach in the EU without prejudice to Member States competences in matters of network roll-out and national security.

17. STRESSES that building trust in 5G technologies is firmly grounded in the core values of the EU such as human rights and fundamental freedoms, rule of law, protection of privacy, personal data and intellectual property, in the commitment to transparency, reliability and inclusion of all stakeholders and citizens, as well as in the enhanced international cooperation.

18. UNDERLINES that the increasingly complex, interconnected and rapidly evolving technology calls for a comprehensive approach and effective and proportionate security measures with focus on security and privacy by design as integral parts of 5G infrastructure and terminal equipment.

19. EMPHASISES that 5G and other related electronic communications networks need to be protected continuously across their entire lifecycle to cover the whole supply chain and all relevant equipment.

20. STRESSES the need to address and mitigate potential challenges arising from the deployment of 5G networks and services to law enforcement including e.g. lawful interception.

21. RECOGNISES the need to put in place robust common security standards and measures, acknowledging international standardization efforts on 5G, for all relevant manufacturers, electronic communications operators and service providers and that key components, such as components critical for national security, will only be sourced from trustworthy parties.

22. SUPPORTS the ongoing work of the European Union Agency for Cybersecurity (ENISA) regarding the European cybersecurity certification framework established by the Cybersecurity Act, with the potential to enhance the level of cybersecurity for ICT products, services and processes.

23. STRESSES that while standardization and certification may be able to address certain security challenges related to 5G networks, additional security measures are required to effectively mitigate the risks.

24. WELCOMES the ongoing preparation by the Commission, in cooperation with Member States and the private sector, of a strategic European partnership on Smart Networks and Services under Horizon Europe with the aim to promote investments, maintain and strengthen competitiveness, reinforce research, innovation and the development of secure solutions in the field of 5G and beyond.

25. WELCOMES the prioritization of cybersecurity in the proposed Digital Europe Programme as a means of reinforcing the EU cybersecurity capacities, as well as the initiative under the proposed Connected Europe Facility program on the 5G TEN-T cross border corridors.

26. CALLS UPON the Member States and the Commission with the support of ENISA to take all necessary measures within their competences to ensure the security and integrity of electronic communication networks, in particular 5G networks, and continue to consolidate a coordinated approach to address the security challenges related to 5G technologies and on the basis of the ongoing joint work on the 5G security toolbox to identify effective common methodologies and tools to mitigate risks related to 5G networks.

_____