European Economic
and Social Committee

TEN/704
Secure 5G deployment – EU toolbox

OPINION

European Economic and Social Committee

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Secure 5G deployment in the EU – Implementing the EU toolbox

[COM(2020) 50 final]

Rapporteur: **Alberto Mazzola**
Co-rapporteur: **Dumitru Fornea**

Referral	European Commission, 09/03/2020
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	03/09/2020
Adopted at plenary	16/09/2020
Plenary session No	554
Outcome of vote (for/against/abstentions)	217/0/2

1. Conclusions and recommendations

1.1 The EESC welcomes the initiative of the Member States and the European Commission to review Member States' progress in implementing the set of key measures recommended in the conclusions of the EU toolbox of strategic and technical measures for the secure deployment of the 5G ecosystem.

1.2 The EESC considers that, in view of the increasing complexity and variety of 5G applications (the Commission has set the following connectivity targets for 2025: schools, universities, research centres, hospitals, main public service providers and digitally intensive enterprises should have access to data upload and download speeds of 1 Gbps; urban and rural households should have access to a download connectivity speed of at least 100 Mbps; urban areas, major roads and railways should have uninterrupted 5G coverage), this review of the 5G ecosystem and the Commission's measures to safeguard the cybersecurity of 5G networks and a diverse 5G value chain, technical standardisation and certification, foreign direct investment, trade defence and competition, public service obligations, procurement and cyber diplomacy should cover geopolitical security, infrastructure and data security and health safety, including pursuant to Article 168(1) TFEU.

1.3 The EESC believes that it is important for the European 5G ecosystem to ensure integrity, confidentiality, management and operational responsibilities, safety, fungibility of supply, interoperability of hardware and software components, common technical standards, continuity of service, flow reliability and data protection, coverage in all areas, including sparsely populated areas, clear communication targeting users as active digital market players, and proactive adherence to the ICNIRP guidelines seeking to protect the health of the population, while reducing radiation as much as possible. Accordingly, ICNIRP has updated the radiofrequency EMF part of the 1998 Guidelines. This document presents these revised guidelines, which provide protection for humans from exposure to EMFs from 100 kHz to 300 GHz.Health Phys. 118(5):483–524; 2020- MARCH 2020. ICNIRP (2020) has made a number of changes to ensure that new technologies such as 5G will not be able to cause harm, regardless of our current expectations.

1.4 The EESC asks the Commission to strictly monitor progress in the deployment and real use of 5G and calls on the Member States to further accelerate the process and ensure a responsible implementation, catering for all safety and security aspects, including those relating to the impact of 5G technology on public health and living ecosystems, the social and economic impact, the impact on competition, education and training, and securing respect for fundamental rights.

1.5 The EESC calls for the EU to be a global leader in the next generation of 5G mobile technology, equipped with secure digital infrastructure as a solid building block of a new, modern European industrial strategy through a radical shift in mobile connectivity and with huge dynamic potential to increase productivity and boost the economy and services for the people.

1.6 In particular, the EESC believes it is vital to assess the risk profile of suppliers and apply relevant restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks and define liabilities – for key assets defined as critical and sensitive in the EU coordinated risk assessment.

1.7 The EESC believes that it is indispensable for Europe to take a medium-term approach to autonomy and self-sufficiency in this field and advocates strongly for research and a range of European companies. The EESC considers it important to increase EU resources for digital R&I and support operator and supplier investment in new technical security functionalities, which should be able to go hand in hand with the ability of the market to recognise and remunerate all initiatives aimed at increasing the security and resilience of systems.

1.8 It is important to ensure security for all Member States, including by maintaining research centres in a variety of areas of the EU: in addition, the EESC reiterates its suggestion of having at least two suppliers for each country, at least one of which is European, in order to ensure political security of data and respect for heath requirements.

1.9 The EESC believes that more attention should be given to instruments for users, citizens and relevant civil society organisations, which are limited and inefficient, in addition to the focus rightly placed on the appropriate measures regarding the power of national regulators and the role of telecommunications operators, with the aim of promoting consumer empowerment, and building consumers' capacity in order to make them proactive market players.

1.10 The Commission, the EP, the Council and the governments and parliaments of the Member States should provide a democratic framework for consultation, where scientific or technological issues, legal guarantees and the responses of the relevant institutions to questions from civil society can be presented to the public.

1.11 The EESC recommends that European technological diplomacy be strengthened to enable the EU to ensure more balanced, reciprocal conditions for trade and investment, in particular as regards market access, subsidies, public procurement, technology transfers, industrial property and social and environmental standards.

2. **Introduction**

2.1 5G network security is an issue of strategic importance for citizens and companies, the entire single market and the EU's technological sovereignty. As early as 2013, the Commission launched the EU flagship initiative setting up a 5G public-private partnership (5G PPP) to speed up research and innovation in 5G technology.

2.2 With worldwide revenues estimated to reach over EUR 100 billion in 2025, 5G is a key asset for Europe to compete in the global market and its cybersecurity is crucial for ensuring the strategic autonomy of the EU.

2.3 5G networks are built on the current 4th generation (4G) of network technologies and on fibre optic infrastructure, providing new service capacities and becoming the central infrastructure and the enabling factor for a large part of the EU’s economy, to form the backbone of a wide range of services essential for the operation of the internal market and for the maintenance and management of vital economic and societal functions, such as energy, transport, banking and health services, and the agricultural and industrial systems of production, distribution and consumption.

2.4 The central role of 5G networks in achieving the digital transformation of the EU economy and society, the interconnected and transnational nature of the infrastructures underpinning the digital ecosystem and the cross-border nature of the threats involved mean that any significant vulnerabilities and/or cybersecurity incidents concerning 5G networks happening in one Member State would affect the Union as a whole. This is why measures should be provided for to underpin a high common level of cybersecurity of 5G networks.

2.5 In 2016, the Commission – in the framework of a set of initiatives starting with the Communication on Connectivity for a Competitive Digital Single Market - Towards a European Gigabit society[1] [2] and including a reform of the regulatory framework for electronic communications[3] and the functions of the Body of European Regulators for Electronic Communications (BEREC)[4], the priorities for ICT standardisation for the digital single market[5] and promotion of internet connectivity in local communities[6] – adopted an EU Action Plan for 5G[7], on which the EESC issued a positive opinion[8], to strengthen the EU's efforts to deploy 5G infrastructure and services in the digital single market with a roadmap for public and private investment in 5G infrastructure in the EU and a target for rolling out 5G commercial networks by 2020.

2.6 According to the definition provided in the Commission Recommendation[9], "5G networks" means "a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices."

2.7 The Recommendation specifies that the Commission will support the implementation of an EU approach on 5G cybersecurity and will act, as requested by Member States, using, where appropriate, all the tools at its disposal to ensure the security of the 5G infrastructure and supply chain:

- telecoms, multimedia and cybersecurity rules;

[1] Article 168(1) TFEU: "Union action, which shall complement national policies ...".

[2] COM(2016) 587.

[3] COM(2016) 590.

[4] COM(2016) 591.

[5] COM(2016) 176.

[6] COM(2016) 589.

[7] COM(2016) 588.

[8] OJ C 125, 21.04.2017, p.74.

[9] Commission Recommendation (EU) 2019/534 of 26.3.2019 on the *Cybersecurity of 5G networks*, OJ L 88, 29.3.2019, p. 42.

- coordination on standardisation as well as EU-wide certification;
- foreign direct investment screening framework to protect the European 5G supply chain;
- trade defence instruments;
- competition rules;
- public procurement, ensuring that due consideration is given to security aspects;
- EU funding programmes, ensuring that beneficiaries comply with relevant security requirements.

2.8 In July 2019, the Member States sent the results of their national risk assessments to the Cooperation Group established by the NIS Directive[10] (made up of representatives of each Member State), the Commission and ENISA, with information on the main activities, threats and vulnerabilities according to standard ISO/IEC 27005 in the area of 5G and the primary risk scenarios, describing the potential ways in which threat actors could exploit the vulnerabilities of an activity: these national assessments were used as the basis for a subsequent coordinated assessment and a joint toolbox of possible risk mitigation measures.

2.9 In October 2019, the NIS Cooperation Group, with the support of the Commission and ENISA, published a report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks, which identified several significant security challenges related to key technological innovations in software, applications and services, and to the role of providers in the deployment and use of 5G networks and the degree of dependence on individual suppliers:

- greater exposure to attacks and an increase in the number of potential access points for the perpetrators of these attacks;
- greater sensitivity arising from the new architectural features and functionalities of 5G networks;
- risks related to the reliance of mobile network operators on suppliers, with an increase in the number of attack paths that could be exploited by threat actors;
- importance of the risk profile of individual suppliers in terms of possible interference from outside the EU;
- greater risks arising from heavy reliance on suppliers in the event of any supply disruptions caused by trade or other tensions;
- threats to the availability and integrity of networks in relation to security, confidentiality and privacy.

2.10 These challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem, and making it essential for Member States to take the necessary mitigating measures.

2.11 On 21 November 2019, ENISA published a report entitled *Threat landscape for 5G networks*, which contains its assessments of the threats linked to fifth generation mobile telecommunications networks and complements the EU Member States' report.

[10] 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.

2.12 On 29 January 2020, the NIS Cooperation Group published the *Cybersecurity of 5G networks – EU toolbox of risk mitigating measures*[11] with a possible common set of measures for mitigating the major cybersecurity risks of 5G networks and providing guidance for the selection of measures that should be prioritised in national and EU mitigation plans. On the same day, the Commission adopted a Communication supporting the toolbox[12], which is the subject of this opinion.

2.13 The main 5G network infrastructure stakeholders are:

- citizens, consumers and end users of 5G;
- mobile network operators (MNOs): entities providing mobile network services to users, managing their network with the help of third parties;
- suppliers of mobile network operators: entities providing services or infrastructure to MNOs to build and/or operate their networks. This category comprises: telecommunications equipment manufacturers; other third party suppliers, such as cloud infrastructure providers, system integrators, security and maintenance contractors and transmission equipment manufacturers;
- manufacturers of connected devices and related service providers: entities that supply objects or services that will be connected to 5G networks (e.g. smartphones, connected vehicles, e-health) and associated service components accommodated by the 5G control plane as defined in the service-based or Mobile Edge Computing architecture;
- other stakeholders, including service and content providers.

All these stakeholders are important stakeholders for security, both in terms of contributing to the cybersecurity of 5G networks and as potential entry points or attack vectors. It is therefore important to assess the risks related to their position in the 5G ecosystem.

2.14 The main conventional kinds of threats are in the area of compromising confidentiality, integrity and availability. More specifically, it was found that a number of threat scenarios for 5G networks concern in particular:

- disruption of the local or global 5G network (availability);
- spying on data traffic in 5G network infrastructure (confidentiality);
- modification or re-routing of data traffic in 5G network infrastructure (integrity and/or confidentiality);
- destruction or alteration of other infrastructure or digital information systems through 5G networks (integrity and/or availability).

2.15 The threats posed by states or state-supported actors are perceived to be of the utmost significance as these are the most serious and most likely threat actors, as they can have the

[11] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[12] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

motivation, intent and, above all, the capability to conduct persistent, sophisticated attacks on the security of 5G networks.

While many of these vulnerabilities are not specific to 5G networks, their number and significance is likely to increase with 5G owing to the increased level of complexity of the technology and greater reliance by economies and societies on this infrastructure in the future.

2.16 In particular, as 5G networks will largely be based on software, the main security flaws, such as those resulting from equipment suppliers' poor software development processes, could make it easier for actors to intentionally insert deliberate backdoors in products and make them also more difficult to detect. This may increase the potential for their use to have a particularly severe and widespread negative impact. While the cybersecurity issues of 4G have not yet been fully resolved, 5G problems might grow exponentially.

2.17 There are also vulnerabilities linked to the process or configuration to be considered:

- lack of specialised and trained staff to protect, monitor and maintain 5G networks;
- inadequate internal security controls, insufficient monitoring practices and safety management systems and weaknesses in risk management practices;
- inadequate security or operating maintenance procedures such as software upgrading/patch management in 5G networks;
- failure to comply with 3GPP standards or incorrect implementation of standards;
- network design or architectural deficiencies, including lack of effective emergency and continuity mechanisms and inadequate or incorrect configuration, for example in virtualisation or administration or access rights;
- inappropriate criteria for local and remote access to network components;
- insufficient security requirements in the supply process: this vulnerability can take the form of inadequate supplier selection strategies or a failure to prioritise security over other aspects.

2.18 Individual suppliers' profiles must be assessed against a number of factors, in particular: the possibility that the supplier will be subject to interference from a non-EU country facilitated by close links between the supplier and the government of a given third country; third-country legislation, in particular where legislative or democratic checks and balances are not in place and where, as a result, the company's subsidiaries operating in the EU might be deterred from following EU legislation, or where there are no security or data protection agreements between the EU and the country in question; the nature of the supplier's corporate ownership structure; the third country's capacity to exert any form of pressure, including with regard to the place where the equipment is manufactured; the general quality of the supplier's cybersecurity practices and products, including the degree of control over its supply chain and whether security practices are prioritised properly.

2.19 Member States have agreed to ensure that measures are put in place to respond adequately and proportionately to the risks identified and possible future risks. In particular, they agreed to ensure that they would be able to restrict, prohibit and/or impose specific requirements and conditions on, under a risk-based approach, the supply, distribution and operation of 5G network equipment.

2.20 To this end, Member States should:

- strengthen security requirements for mobile network operators such as strict access controls, rules on secure operating and monitoring, and limitations on outsourcing of specific functions;
- assess the risk profile of suppliers on the basis of objective and clear criteria; as a consequence, apply relevant restrictions following the principles of proportionality and legal certainty for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks – for key assets defined as critical and sensitive in the EU coordinated risk assessment;
- enact globally recognised and implemented and consensus-based security standards and best practices;
- ensure that each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier or suppliers with a similar risk profile;
- ensure strict access control and secure network management, operation and monitoring, and use certification for 5G network components and/or processes. This strategy needs to be based on a risk analysis conducted by Member States and operators, so that the choice of a multi-vendor strategy does not increase the risk level for the operator's network;
- ensure an adequate balance of suppliers at national level and avoid dependency on suppliers considered to be high risk, including by promoting greater interoperability of equipment;
- maintain a diverse and sustainable 5G supply chain in order to avoid long-term dependency by making full use of EU foreign direct investment screening instruments, trade defence instruments, competition rules and EU procurement rules;
- strengthen EU internal capacities in 5G and post-5G technologies, by using relevant EU programmes and funding, and ensure coordination between Member States on standardisation through enhanced "testing" and "auditing" capabilities, to meet specific security objectives and develop relevant EU certification schemes under the Cybersecurity Act and promote interoperability.

2.21 As repeatedly pointed out by the Commission, the European internal market is and remains open to people wishing to come to Europe, as long as they all comply with clear, demanding rules based on objective criteria.

2.22 On 6 June 2020, the Council underlined the importance of strengthening digital sovereignty and cooperation in the EU and creating synergies through EU programmes such as the Connecting Europe Facility and the Digital Europe Programme, with the development of digital skills and the development of the data economy, and the importance of artificial intelligence and cybersecurity, with the digital sector having an active role to play in achieving the goals of the Green Deal.

3. The Commission Communication

3.1 In response to the NIS Cooperation Group's 5G security toolbox, the Commission:

- is undertaking to act, as requested by Member States, using, where appropriate, all the tools at its disposal to ensure the security of the 5G infrastructure and supply chain;
- is calling on the Member States to ensure implementation of effective risk mitigating strategies, and to take further steps to ensure coordination at EU level for a concerted approach to the security of 5G networks;
- is asking the Member States to implement the set of measures recommended in the conclusions of the EU toolbox and to prepare a joint report on their implementation while the NIS Cooperation Group continues to work to support the implementation of the toolbox;
- has set out – in the sectors within its remit – measures safeguarding the cybersecurity of 5G networks and a diverse 5G value chain, technical standardisation and certification, foreign direct investment, trade defence and competition, procurement and cyber diplomacy, as well as its relevant programmes and funds dedicated to R&I, cohesion and development.

4. General comments

4.1 The EESC firmly believes that the new 5G technologies can change the way we interact with the world, offering opportunities for new applications, business models, new lifestyles, smart factories, greater productivity and new quality services for people, potentially opening doors to breakthrough technologies such as automated cars and advanced manufacturing and distribution systems, as well as making possible many thousands of interconnected devices set to enter our daily lives as part of the Internet of Things (IoT). However, the EESC would expect the EC to strengthen the impact and feasibility studies and the cost-benefit analysis of 5G compared to the use of 4G technology or fibre optic telecommunications. The EESC considers it essential that 5G is oriented to achieve a better circular use of resources and to reduce the large energy-related CO_2 footprint. The EESC highlights the importance of dealing with social structural changes by enhancing a fair and smooth transition and addressing the skills gap to get to better paid, flexible, highly skilled jobs.

4.2 This triple threat – uncontrolled pandemics, inadequate economic policy toolboxes and geopolitical "black swans" – could push the global economy into a lasting depression and financial market crashes and capital flight, just when all sections of European society are becoming increasingly aware that sustainable economic development **and the current digital revolution – of which 5G is a cornerstone** – require ways of simultaneously combining technological sovereignty, productivity gains and a more efficient use of the available resources supported by a suitable legal and regulatory framework and economic and financial framework.

4.3 The EESC calls on the EU and the Member States to complete the digital single market, including by developing capacities to integrate 5G services and use them to defend and improve the competitiveness of European industries: it asks the Commission to strictly monitor progress in the deployment and real use of 5G and calls on the Member States to further accelerate the process, catering for all safety and security aspects, including those relating to the impact of 5G technology on public health and living ecosystems, the social and economic impact, the impact on competition, education and training, and securing respect for fundamental rights, such as the right to ownership or the right to privacy and personal data security.

4.4 The EESC calls for the EU to be a global leader in the next generation of 5G mobile technology, equipped with secure digital infrastructure as a solid building block of a new, modern European industrial strategy through a radical shift in mobile connectivity and with huge dynamic potential to increase productivity and boost the economy and services for the people, their well-being and climate and environmental protection by placing the EU at the forefront of the 5G revolution.

4.5 Given that cybersecurity and national security are inextricably linked, the EESC believes that any decision on the national security of an EU Member State must be taken in the EU context, and that non-technical evaluations should be implemented objectively on the basis of risk assessment criteria defined at European level necessary to provide a harmonised and predictable regulatory environment across Europe that ensures full interoperability.

4.6 The EESC believes that the quality of information and the ways in which it is conveyed – the so-called framing effect or salience – has a significant influence on the behaviour of the addressees. The objective of promoting consumer empowerment is therefore reflected in the identification of tools for educating consumers and building their capacity to make them active players on the digital market. The EESC recognises the need to provide people with up-to-date, accurate information on the benefits and risks of 5G based on the consensus of the vast majority of the scientific community, pointing out the aspects on which such consensus is uncertain.

4.7 The EESC firmly believes that access to the European digital market must continue to be open to any undertaking without discrimination, but within the European framework of rules, standards and firm, clear assessment and security criteria putting the recovery and revival of European technological sovereignty back at the heart of the European strategy.

4.8 Although the five major vendors of infrastructure include two European suppliers, two Chinese, and one Korean[13], no major European company is among the first to produce 5G devices and chipsets; the EESC firmly believes that a range of different suppliers must be ensured, at least one of which is owned by a European parent company, along with a framework for interoperability and full interchangeability of hardware and software components, not least to ensure full European technological sovereignty in the context of strong international cooperation and full mutual openness, access and operability in the markets. Such diversification may be applied as long as interoperability of the services is possible and the cybersecurity risks are not increased as a result of the diversity.

4.9 The EESC believes that it is indispensable for Europe to take a medium-term approach to autonomy and self-sufficiency in this field and advocates strongly for research and a range of European companies. The EESC welcomes the package of measures agreed by the Member States to address security and safety risks related to the introduction of 5G technology which have already been identified by the European assessment. It considers, however, that the

[13] The current five main global suppliers are: Ericsson, Nokia, Huawei, ZTE and Samsung.

stringent, safe exposure limits for electromagnetic fields, as recommended at EU level and based on updated guidance from the International Commission on Non-Ionizing Radiation Protection (ICNIRP), recognised by the World Health Organization (WHO), should apply to all frequency bands designated for 5G[14]: the ICNIRP limits are based on the precautionary principle as they are 50 times lower than the public health impact levels established on the basis of the available scientific evidence.

4.10 However, the EESC notes that ICNIRP are not recognised by all the community, with some scientists promoting much stricter population exposure limits according to the ALARA principle. The solutions that might be proposed to complement the 5G communications infrastructure includes the use of fixed data connections by existing non-radio technologies (Ethernet cables, fibre optics, etc.), in situations where the use is fixed (e.g. ATMs, banking POS, industrial robots, remote controlled medical robots, etc.) and where large data transmission users operate (digital service providers, companies/ businesses, etc.); IoT Internet of Things present in fixed, non-mobile locations (Smart Home, Smart City, sensors on public utility equipment, etc.).

4.11 The Commission, the EP, the Council and the governments and parliaments of the Member States should provide a democratic framework for consultation, where scientific or technological issues, legal guarantees and the responses of the relevant institutions to questions from civil society can be presented to the public.

4.12 The EESC believes that more attention should be given to instruments for users, citizens and relevant civil society organisations, which are limited and inefficient, in addition to the focus rightly placed on the appropriate measures on the power of national regulators and the role of telecommunications operators.

4.13 The EESC has acknowledged[15] and is concerned about the problem of electromagnetic hypersensitivity (EHS) and highlighted its concerns; it is encouraged to note that further substantial research is ongoing to understand the problem and its causes, and urges the Commission to continue and update its work in this field.

4.14 The credibility of 5G telecommunications and application service providers is essential, in the EESC's view, as online information management is the basis of data aggregation services for data collected and processed by users, through technological, legal and tax mechanisms, interlinking objects, machines and algorithms.

4.15 The EESC has suggested[16] moving from data ownership concepts to a definition of data rights for individuals and legal persons. Consumers should be in control of the data produced by connected devices in a way that ensures consumer privacy along with accessibility,

[14] EP — E-003040/2019 Answer given by Ms Kyriakides on behalf of the European Commission (17.1.2020).

[15] OJ C 242, 02.07.2015, p.31.

[16] OJ C 353, 18.10.2019, p.79.

interoperability and data transfer, while ensuring adequate data protection and confidentiality, fair competition and a wider choice for consumers.

4.16 The General Data Protection Regulation (GDPR) should be supplemented with clear implementation guidelines in order to achieve uniform implementation and a high level of data and consumer protection in view of the interconnectivity of machines and objects, and the rules on civil liability and product insurance should be revised to cater for a situation where decisions will increasingly be taken by software in a fully secure environment.

4.17 The EESC considers it essential that Member States follow the strategic and technical recommendations in the EU toolbox, avoiding the development of specific national approaches, such as additional testing and certification that would lead to market fragmentation, delays in the implementation of technologies and inconsistencies between markets, with the risk of undermining confidence in testing and certification systems.

4.18 The EESC considers it essential to make use of global standards, with greater European support, and of consensual, recognised best practices in order to achieve efficient management of threats, generate economies of scale, avoid fragmentation and guarantee the interoperability of European systems. The conversations on technical standards are a necessary clarification that will allow companies to compete once again and to carry out these key activities in order to implement advanced technologies such as 5G and artificial intelligence (AI) in all markets.

4.19 In particular, the EESC believes it is vital to assess the risk profile of suppliers and apply relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets defined as critical and sensitive in the EU coordinated risk assessment.

4.20 The EESC considers it important to increase operator and supplier investment in new technical security functionalities, which should be able to go hand in hand with the ability of the market to recognise and remunerate all initiatives aimed at increasing the security and resilience of systems. More focus on security investments could bring new market rewards.

4.21 The EESC is strongly in favour of joint measures to support industrial development and 5G deployment: evaluation of potential market gaps or failures along the 5G value chain, which would justify targeted interventions under the next long-term budget or a possible project of common European interest on 5G cybersecurity (security and safety).

4.22 The EESC stresses that, while digital infrastructure has proved to be resilient and robust during the COVID-19 crisis, further investment in 5G infrastructure is needed in order to overcome a persisting digital divide that can limit people's access to e-health, e-learning and remote working.

4.23 In terms of technological diplomacy, the EESC considers it essential that the EU ensure more balanced, reciprocal conditions for trade and investment, in particular as regards market access, subsidies, public procurement, technology transfers, industrial property and social and environmental standards, especially given the existence of "systemic rivals promoting alternative models of governance", while encouraging full competition and technical innovation in the market.

4.24 The EESC firmly supports the need to maintain a diversified, sustainable 5G supply chain in order to avoid long-term dependence by requiring multiple suppliers to be used in a framework of interchangeability and interoperability, and to further strengthen the 2021-2027 financial framework for capacity-building programmes and initiatives and European 5G and post-5G technological sovereignty.

4.25 In the context of the recovery plan for Europe adopted on 27 May 2020, the 2020 Digital Economy and Society Index (DESI) will inform the country-specific analysis supporting the European Semester's digital recommendations. This will help Member States to target and prioritise their reform and investment needs, thereby facilitating access to the EUR 560 billion Recovery and Resilience Facility. The Facility will provide Member States with the funds to make their economies more resilient and ensure that investments and reforms support the green and digital transitions. As the pandemic had a significant impact on each of the five DESI dimensions, the 2020 conclusions on 5G should be viewed alongside the numerous measures adopted by the Commission and the Member States to manage the crisis and to support the recovery.

Brussels, 16 September 2020

Luca JAHIER
The president of the European Economic and Social Committee

____