RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2019/534

of 26 March 2019

Cybersecurity of 5G networks

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The Commission has recognised 5th generation (5G) deployment of network technologies as a major enabler for future digital services and a priority for the Digital Single Market strategy. The Commission adopted the 5G Action Plan to make sure that the Union has the connectivity infrastructure necessary for its digital transformation from 2020 ([1]).

(2) 5G networks will build on the current 4th generation (4G) of network technologies, by providing new service capabilities and becoming the central infrastructure and enabler for large parts of the Union economy. Once rolled out, 5G networks will form the backbone for a wide range of services essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions – such as energy, transport, banking, and health, as well as industrial control systems. The organisation of democratic processes, such elections, will also rely more and more on digital infrastructure and 5G networks.

(3) The dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious. As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union, at a time when cyber-attacks are on the rise and more sophisticated than ever.

(4) 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 to underpin a high common level of cybersecurity of 5G networks.

(5) The need for action at Union level has been confirmed by the Member States. In its conclusions of 21 March 2019, the European Council looked forward to a Commission recommendation on a concerted approach to the security of 5G networks ([2]).

(6) Ensuring European sovereignty should be a major objective, in full respect of Europe's values of openness and tolerance ([3]). Foreign investment in strategic sectors, acquisition of critical assets, technologies and infrastructure in the Union and supply of critical equipment may also pose risks to the Union's security.

(7) The cybersecurity of 5G networks is key for ensuring the strategic autonomy of the Union, as recognised in the Joint Communication 'EU-China, a Strategic Outlook' ([4]).

(8) The European Parliament's resolution on security threats connected with the rising Chinese technological presence in the Union also calls on the Commission and Member States to take action at Union level ([5]).

(9) This Recommendation addresses cybersecurity risks in 5G networks by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk assessment and on establishing a process to develop a common toolbox of best risk management measures.

(10) There is a strong Union legislative framework in place to protect electronic communications networks.

([1]) COM(2016)588 final.
([2]) European Council conclusions of 21 and 22 March 2019.
([3]) State of the Union 2018 – The Hour of European Sovereignty, 12 September 2018.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//EN.

(11) The Union's framework in the field of electronic communications ([6]) promotes competition, internal market and end-user interests and with the European Electronic Communications Code ([7]) pursues an additional connectivity objective, articulated in terms of outcomes: widespread access to and take-up of very high capacity fixed and mobile connectivity for all Union citizens and businesses while safeguarding the interests of the citizens. Directive 2002/21/EC requires Member States to ensure that the integrity and security of public communications networks are maintained, with obligations to ensure that undertakings providing public communications networks or publicly available electronic communications services take technical and organisational measures to appropriately manage the risks posed to security of networks and services. It also provides that competent national regulatory authorities have powers, including the power to issue binding instructions, to ensure compliance with such obligations.

(12) In addition, Directive 2002/20/EC of the European Parliament and of the Council ([8]) allows Member States to attach conditions concerning the security of public networks against unauthorised access to the general authorisation, for the purpose of protecting the confidentiality of communications in accordance with Directive 2002/58/EC of the European Parliament and of the Council ([9]).

(13) To support the implementation of these obligations, the Union has set up a number of cooperation bodies. The Agency for Network and Information Security (ENISA), the Commission, Member States and national regulatory authorities have developed technical guidelines for national regulatory authorities on incident reporting, security measures and threats and assets ([10]). The Cooperation Group established by Directive (EU) 2016/1148 of the European Parliament and of the Council ([11]) ('the Cooperation Group') brings together competent authorities in order to support and facilitate cooperation, in particular by providing strategic guidance for the activities of the Computer Security Incident Response Teams network, which at technical level facilitates operational cooperation.

(14) The future European cybersecurity certification framework ([12]) should provide an essential supporting tool to promote consistent levels of security. It should allow for the development of cybersecurity certification schemes to respond to the needs of users of 5G-related equipment and software. The critical importance of these infrastructures should make the development of relevant European cybersecurity certification schemes for information and communications technologies' products, services or processes used for 5G networks an immediate priority. Member States and market players should actively engage in the development of such certification schemes, including providing support for the definition of specific protection profiles for 5G networks.

(15) In the absence of harmonised Union law, Member States may specify by means of national technical regulations, adopted in compliance with Union law, that a European cybersecurity certification scheme should be mandatory. Member States also have recourse to European cybersecurity certification schemes in the context of public procurement and of Directive 2014/24/EU of the European Parliament and of the Council ([13]) and could support the development of assistance mechanisms – such as an assistance hub – for the purchase of cybersecurity solutions by public buyers.

(16) A high level of data protection and privacy is an important element in ensuring the security of 5G networks. Rules have also been defined at Union level ensuring the security of processing of personal data, including in electronic communications. The General Data Protection Regulation ([14]) sets the obligation to process personal data in a manner that ensures its security, including for preventing unauthorised access to or use of personal data and the equipment used for the processing. The Directive on privacy and electronic communications lays down

([6]) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33) and the Specific Directives.

([7]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

([8]) Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p. 21).

([9]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) 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 (OJ L 194, 19.7.2016, p. 1).

([12]) Proposal for a Regulation of the European Parliament and Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification 'Cybersecurity Act' (COM(2017) 477 final — 2017/0225 (COD).

([13]) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

([14]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

specific rules on the protection of confidentiality of communications and of the terminal equipment of end-users. It also imposes obligations on service providers to take appropriate technical and organisational measures to safeguard the security of their services.

(17) The Union has also adopted an instrument that will protect critical infrastructure and technologies, such as those used in communications, by allowing Member States to screen foreign direct investments on grounds of security or public order and by creating a cooperation mechanism where Member States and the Commission will be able to exchange information and raise concerns related to specific investments ([15]).

(18) Member States and operators are currently taking important preparatory steps towards enabling the large-scale roll-out of 5G networks. Several Member States have expressed concerns about potential security risks related to 5G networks in the context of carrying out procedures for the grant of rights of use in radio spectrum bands designated for 5G networks ([16]) — and have been exploring measures to address these risks.

(19) Addressing cybersecurity risks in 5G networks should take into account both technical and other factors. Technical factors may include cybersecurity vulnerabilities that may be exploited to gain unauthorised access to information (cyberespionage, be it for economic or political reasons) or for other malicious purposes (cyberattacks aimed at disrupting or destroying systems and data). Important aspects to consider should be the need to protect the networks across their entire lifecycle and the need to cover all relevant equipment, including in the design, development, procurement, deployment, operation and maintenance phases of 5G networks.

(20) Other factors may include regulatory or other requirements imposed on information and communications technologies equipment suppliers. An assessment of the significance of such factors would need to take into account, inter alia, the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection between the Union and the third country concerned, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection.

(21) As an important step in developing a Union approach to the cybersecurity of 5G networks, a risk assessment should be conducted and completed at national level. This would help Member States to adapt national measures on security requirements and risk management in the light of this assessment.

(22) Coordination should be developed to ensure the effectiveness of measures aimed at addressing these cybersecurity threats, measures which are essential for the smooth functioning of the internal market and for the protection of personal data and privacy.

(23) The national risk assessments should form the basis for a coordinated Union risk assessment, made up of a threat landscape mapping and a joint review to be conducted by the Member States, with support from the Commission and together with the European Agency for the Cybersecurity (ENISA).

(24) Taking into account national and Union risk assessments, the Cooperation Group should establish a toolbox identifying types of cybersecurity risk and of possible measures to mitigate the risks in areas including certification, testing and access controls. It should also identify possible specific measures appropriate to address risks identified by one or more Member States. The Cooperation Group should draw on the support of the European Agency for Cybersecurity (ENISA), Europol, the Body of European Regulators for Electronic Communications (BEREC) and the EU Intelligence and Situation Centre. This toolbox should serve to advise the Commission on developing minimum common requirements to further ensure a high level of cybersecurity of 5G networks across the Union.

(25) When measures are taken to address cybersecurity risks consideration should be given to the promotion of cybersecurity through diversity of suppliers when building any single network.

([15]) Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I, 21.3.2019, p. 1).

([16]) The auction procedure in at least one spectrum band is scheduled for 2019 in 11 Member States: Austria, Belgium, Czechia, France, Germany, Greece, Hungary, Ireland, Netherlands, Lithuania, Portugal. Six more auctions are scheduled for 2020: Spain, Malta, Lithuania (different frequencies), Slovakia, Poland, UK. Source: http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) This Recommendation should be without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law, including the right of the Member States to exclude providers or suppliers from their markets for national security reasons.

HAS ADOPTED THIS RECOMMENDATION:

I. **OBJECTIVES**

(1) In order to support the development of a Union approach to ensuring the cybersecurity of 5G networks, this recommendation identifies the actions which should be taken to enable:

(a) Member States to assess the cybersecurity risks affecting 5G networks at national level and take necessary security measures.

(b) Member States and relevant Union institutions, agencies and other bodies to develop jointly a coordinated Union risk assessment that builds on the national risk assessment.

(c) The Cooperation Group set up under Directive (EU) 2016/1148 (Cooperation Group) to identify a possible common set of measures to be taken to mitigate cybersecurity risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks.

II. **DEFINITIONS**

(2) For the purposes of this Recommendation:

(a) '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. These may include legacy network elements based on previous generations of mobile and wireless communications technology such 4G or 3G. 5G networks should be understood to include all relevant parts of the network.

(b) 'infrastructures underpinning the digital ecosystem' means infrastructures used to enable digitisation across a wide range of critical applications in economy and society.

III. **ACTION AT NATIONAL LEVEL**

(3) By 30 June 2019, Member States should carry out a risk assessment of the 5G network infrastructure, including identifying the most sensitive elements where security breaches would have a significant negative impact. By the same date, Member States should also review the security requirements and the risk management methods applicable at national level, to take into account cybersecurity threats that may arise from (i) technical factors, such as the specific technical characteristics of 5G networks, and (ii) other factors such as the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries.

(4) On the basis of this national risk assessment and review and taking into account ongoing coordinated action at Union level, Member States should:

(a) update the security requirements and the risk management methods applied in regard to 5G networks;

(b) update the relevant obligations imposed on undertakings providing public communications networks or publicly available electronic communications services pursuant to Articles 13a and 13b of Directive 2002/21/EC;

(c) attach conditions to the general authorisation concerning the security of public networks against unauthorised access and ask for commitments from the undertakings participating in any upcoming procedures for granting rights of use for radio frequencies in 5G bands as regards compliance with security requirements for networks pursuant to Directive 2002/20/EC;

(d) apply other preventive measures aimed at mitigating potential cybersecurity risks.

(5) Measures referred to under point 4 should include reinforced obligations on suppliers and operators to ensure the security of sensitive parts of the networks as well as,, obligations, where appropriate, such as the provision of relevant information to competent national authorities concerning planned changes in electronic communications networks and requirements to have specific information technology components and systems tested in advance for security and integrity purposes by national auditing/certification laboratories.

(6) Joint security reviews should be conducted by two or more Member States, using and sharing the appropriate technical expertise and facilities relating to infrastructures underpinning the digital ecosystem and 5G networks, for example when the same undertaking is operating or building network infrastructure in more than one Member State or where there are major similarities in network configurations. The European Agency for Cybersecurity (ENISA), Europol and the Body of European Regulators for Electronic Communications (BEREC) should give priority to requests for support from Member States in this area. The results of these reviews should be transmitted to the Cooperation Group and the Computer Security Incident Response Team Network.

IV. **COORDINATED ACTION AT UNION LEVEL**

(7) In order to develop a common approach to address the cybersecurity risks in regard to 5G networks Member States should start operating within a dedicated work stream in the Cooperation Group by 30 April 2019. Member States should invite relevant authorities to participate, when appropriate, to the work of the Cooperation Group.

A coordinated European risk assessment

(8) Member States should exchange information with each other and with relevant Union bodies for the purpose of building a common awareness of the existing and potential cybersecurity risks associated with 5G networks.

(9) Member States should transmit their national risk assessments to the Commission and to the European Agency for Cybersecurity (ENISA) by 15 July 2019.

(10) The European Agency for Cybersecurity (ENISA) should complete a specific 5G networks threat landscape mapping. The Cooperation Group and the Computer Security Incident Response Teams network set up under Directive (EU) 2016/1148 should support this process.

(11) Taking into account all these elements and by 1 October 2019, Member States with the support of the Commission and together with the European Agency for Cybersecurity (ENISA) should complete a joint review of the Union-wide exposure to risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks.

(12) This joint review should prioritise an analysis of the risks applicable to the particularly sensitive or vulnerable elements included in the core elements of the 5G networks, to the operations and maintenance centre, as well as to the 5G access network elements used for industrial applications.

(13) In a second phase, this joint review should be extended to other strategic elements of the digital value chain.

A common Union toolbox to address the risks

(14) The work of the Cooperation Group should identify best practices measures applied at national level of the type foreseen in point 4. On the basis of these national best practices, a toolbox of appropriate, effective and proportionate possible risk management measures to mitigate the identified cybersecurity risks at national and Union level should be agreed by 31 December 2019, for advising the Commission on developing minimum common requirements to further ensure a high level of cybersecurity of 5G networks across the Union.

(15) This toolbox should include:

(a) an inventory of the types of security risks that can affect the cybersecurity of 5G networks (e.g. supply chain risk, software vulnerability risk, access control risk, risks arising from the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries); and

(b) a set of possible mitigating measures (e.g. third-party certification for hardware, software or services, formal hardware and software tests or conformity checks, processes to ensure access controls exist and are enforced, identifying products, services or suppliers that are considered potentially not secure, etc.). These measures should address every type of security risk identified in one or more Member States following the risk assessment.

(16) Once European cybersecurity certification schemes relevant for 5G networks are developed, Member States should adopt, in compliance with Union law, national technical regulations providing for mandatory certification of information and communications technologies products, services or systems covered by these schemes.

(17) Member States, together with the Commission, should identify the conditions concerning the security of public networks against unauthorised access to be attached to the general authorisation and security requirements for networks for the purposes of asking commitments from the undertakings participating in procedures for granting rights of use of spectrum in 5G bands pursuant to Directive 2002/20/EC. These should be reflected, where possible, in measures taken in point 4(c).

(18) Member States should cooperate with the Commission to develop specific security requirements that could apply in the context of public procurement related to 5G networks. This should include mandatory requirements to implement cybersecurity certification schemes in public procurement insofar as such schemes are not yet binding for all suppliers and operators.

V. **REVIEW**

(19) Member States should cooperate with the Commission to assess the effects of this Recommendation by 1 October 2020, with a view to determine appropriate ways forward. This assessment should take into account the outcome of the coordinated Union risk assessment and the Union toolbox.

Done at Strasbourg, 26 March 2019.

For the Commission
Julian KING
Member of the Commission