Questions and Answers – Commission recommends common EU approach to the security of 5G networks

Why is the roll out of 5G networks crucial for Europe?

Fifth generation (5G) networks will form the future backbone of our societies and economies, connecting billions of objects and systems, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Democratic processes, such as elections, increasingly rely on digital infrastructures and 5G networks, highlighting the need to address any vulnerabilities and making the Recommendation presented today by the Commission all the more pertinent ahead of the European Parliament elections in May.

5G is also a key asset for Europe to compete in the global market. Worldwide 5G revenues should reach the equivalent of €225 billion in 2025. Benefits of 5G introduction across four key industrial sectors, namely automotive, health, transport and energy, may reach €114 billion per year.

5G roll out is under the responsibility of the Member States. Together with operators, EU countries are currently taking important steps to prepare it. For 2019, the auction procedure in at least one spectrum band is scheduled in 11 Member States: Austria, Belgium, Czech Republic, France, Germany, Greece, Hungary, Ireland, Netherlands, Lithuania, and Portugal. Six more auctions are scheduled for 2020 in Spain, Malta, Lithuania, Slovakia, Poland, and the UK.

At EU level, the 5G Action Plan sets the target dates of 2020 for commercial launch in all Member States and 2025 for comprehensive roll-out in cities and along major transport paths. The latest report from the Commission's 5G Observatory shows that European operators are competing with other leading world regions as they prepare for the commercial launch of 5G this year. Europe is a world leader in 5G trial activities, mainly thanks to the Commission's 5G Public-Private Partnership, with 139 trials, mainly in key vertical sectors, reported in 23 Member States.

The European Electronic Communications Code will support the deployment and take-up of 5G networks, notably as regards assignment of radio spectrum, investment incentives and favourable framework conditions, while the recently adopted rules on open Internet provide legal certainty as regards the deployment of 5G applications. On the private side, market players are planning their infrastructure investment and setting up partnerships for taking the technology solutions from the trial phase to commercial deployment.

Why the risks related to future 5G networks need to be assessed?

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 as elections, will also rely more and more on digital infrastructure and 5G networks.

Any vulnerability in 5G networks could be exploited in order to compromise such systems and digital infrastructure – potentially causing very serious damage or in order to conduct large-scale data theft or espionage. The dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious. This justifies the need for a robust risk-based approach, rather than one relying primarily on ex-post mitigation measures.

Member States have expressed concerns about potential security risks related to 5G networks and have been exploring or taking measures to address these risks, as well as stating that they were looking forward to a common approach at EU level in the conclusions of the European Council of 22 March 2019.

Why do we need to act at European level to secure 5G networks?

The interconnected and transnational nature of the digital infrastructures and the cross-border nature of the threats involved, mean that any vulnerability in 5G networks or a cyber-attack targeting the future networks in one Member State would affect the Union as a whole. This is why concerted measures taken both at national and European levels must ensure a high level of cybersecurity.

Ensuring the cybersecurity of 5G networks is an issue of strategic importance for the EU, at a time when cyber-attacks are on the rise and more sophisticated than ever, and when the need to protect human rights and fundamental freedoms online becomes increasingly important.

At their meeting of 22 March 2019, the EU Heads of State or Government stated that they were looking forward to the Commission recommending a concerted approach to the security of 5G networks. 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.

Furthermore, 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". Foreign investment in strategic sectors, acquisitions of critical assets, technologies and infrastructure in the EU, involvement in EU standard-setting and supply of critical equipment can pose risks to the EU's security. This is particularly relevant for critical infrastructure, such as 5G networks that will be essential for our future and need to be fully secure.

How will the EU coordination work? What are the necessary steps?

1. At national level

Each Member State should complete a national risk assessment of 5G network infrastructures by the end of June 2019. On this basis, Member States should update existing security requirements for network providers and include conditions for ensuring the security of public networks, especially when granting rights of use for radio frequencies in 5G bands. These measures should include reinforced obligations on suppliers and operators to ensure the security of the networks. The national risk assessments and measures should consider various risk factors, such as technical risks and risks linked to the behaviour of suppliers or operators, including those from third countries. National risk assessments will be a central element towards building a coordinated EU risk assessment.

EU Member States have the right to exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework.

2. At EU level

Member States should exchange information with each other and with the support of the Commission and the European Agency for Cybersecurity (ENISA), will complete a coordinated risk assessment by 1 October 2019. On that basis, Member States will agree on a set of mitigating measures that can be used at national level. These can include certification requirements, tests, controls, as well as the identification of products or suppliers that are considered potentially non-secure. This work will be done by the Cooperation Group of competent authorities, as set out under the Directive on Security of Network and Information Systems, with the help of the Commission and ENISA. This coordinated work should support Member States' actions at national level and provide guidance to the Commission for possible further steps at EU level. In addition, Member States should develop specific security requirements that could apply in the context of public procurement related to 5G networks, including mandatory requirements to implement cybersecurity certification schemes.

Today's Recommendation will make use of the **wide-range of instruments** already in place or agreed to reinforce cooperation against cyber-attacks and enable the EU to act collectively in protecting its economy and society, including the first EU-wide legislation on cybersecurity (Directive on Security of Network and Information Systems), the Cybersecurity Act recently approved by the European Parliament, and the new telecoms rules.

The Recommendation will also help Member States to implement these new instruments in a coherent manner when it comes to 5G security.

What EU legislation is already in place or is being implemented to protect future 5G networks?

The EU has a **range of instruments** to protect electronic communications networks, including the first EU-wide legislation on cybersecurity (Directive on Security of Network and Information Systems), the Cybersecurity Act

recently approved by the European Parliament, and the new telecoms rules.

In addition, EU Member States can exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework.

Rules in the field of telecoms: Member States have to ensure that the integrity and security of public communications networks are maintained, with obligations to ensure that operators take technical and organisational measures to appropriately manage any risks to the security of networks and services. It also provides that competent national regulatory authorities have powers, including the power to issue binding instructions and ensure compliance with them. In addition, Member States are allowed 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.

Tools in the field of cybersecurity: The future European cybersecurity certification framework for digital products, processes and services, which was recently agreed by the European Parliament, 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.

To support the implementation of these obligations and instruments, the Union has set up a number of cooperation bodies. The European Agency for Cybersecurity (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. The Cooperation Group established by the Directive on Security of Network and Information Systems brings together competent authorities in order to support and facilitate cooperation, in particular by providing strategic guidance.

Ensuring cybersecurity also requires maintaining a sufficient level strategic autonomy, through achieving a critical mass of investment in cybersecurity and advanced digital technologies in the EU. The Commission therefore proposed making this objective a priority in the next EU budget period, notably through its proposal for a Digital Europe Programme, and proposed a new European Cybersecurity Competence Centre and network to implement relevant projects in the area of cybersecurity.

Rules in the field of public procurement: EU rules on public procurement help obtain better value for taxpayer money by ensuring that public contracts are awarded through competitive, open, transparent and well-regulated tender procedures.

EU public procurement directives do not differentiate between EU and non-EU economic operators but include a number of safeguards. For example, they allow contracting authorities to reject under certain conditions tenders that are unjustifiably low or that do not respect of security, labour and environmental standards. They also allow contacting authorities to protect their essential security and defence interests.

Rules on screening foreign direct investment: The new Regulation will enter into force in April 2019 and will fully apply from November 2020. It will provide a powerful instrument to detect and raise awareness of foreign investment in critical assets, technologies and infrastructure. It will further allow security and public order threats posed by acquisitions in sensitive sectors to be collectively identified and addressed. Member States should use the period between entry into force and the start of application of the Regulation to make the necessary changes to their national domestic practices and legislation and put in place the administrative structures to ensure effective cooperation at EU level with the Commission in accordance with the established mechanisms.

Horizontal sanctions regime to counter cyber-attacks: Proposed by the Commission and the High Representative, the new regime will have worldwide coverage and will enable a flexible EU response irrespective of the location from where cyber-attacks are launched and regardless of whether they are carried out by state or non-state actors. This sanctions regime, when adopted, would enable the Union to respond to cyber-attacks with a 'significant effect', which threaten the integrity and security of the EU, its Member States and our citizens.

What is the role of the European Agency for Cybersecurity in this coordination?

The Cybersecurity Act, recently approved by the European Parliament, gives a permanent and stronger mandate to the European Agency for Cybersecurity (European Network and Information Security Agency-ENISA).

ENISA is already providing support to the Commission in the area of security of telecommunications networks. Together with Member States and national regulatory authorities, ENISA has developed technical guidelines for national regulatory authorities on incident reporting, security measures and threats and assets.

In addition, the Recommendation asks ENISA to provide support for the development of a coordinated EU risk assessment on 5G networks.

ENISA will also work towards the development of Europe-wide certification schemes, as foreseen in the Cybersecurity Act.

What are the next steps?

- Member States should complete their national risk assessments by **30 June 2019** and update necessary security measures. The national risk assessment should be transmitted to the Commission and European Agency for Cybersecurity by **15 July 2019**.
- In parallel, Member States and the Commission will start coordination work within the Cooperation Group set up under the Directive on Security of Network and Information Systems. ENISA will complete a 5G threat landscape that will support Member States in the delivery by **1 October 2019** of the EU-wide risk assessment.
- By **31 December 2019**, the Cooperation Group should agree on a toolbox of

mitigating measures to address the identified cybersecurity risks at national and Union level.

- Once the Cybersecurity Act, recently approved by the European Parliament, enters into force in the coming weeks, the Commission and ENISA will take all necessary steps to set up the EU-wide certification framework. Member States are encouraged to cooperate with the Commission and ENISA to prioritise a certification scheme covering 5G networks and equipment.
- By **1 October 2020,** Member States – in cooperation with the Commission – should assess the effects of the Recommendation in order to determine whether there is a need for further action. This assessment should take into account the outcome of the coordinated European risk assessment and of the effectiveness of the measures.

For More Information

Recommendation on Cybersecurity of 5G Networks

Press release

Security Union: 15 out of 22 legislative initiatives agreed so far

Press release: EU negotiators agree on strengthening Europe's cybersecurity

5G Action Plan

Press release: Joint Communication 'EU-China – A Strategic Outlook'