Secure 5G networks: Questions and Answers on the EU toolbox

Brussels, 29 January 2020

Why is the cybersecurity of 5G networks important?

As a major enabler for future digital services, 5G will play a key role in the development of our digital economy and society in the years to come. From personalised medicine to precision agriculture, from smart energy grids to connected mobility, 5G will potentially affect almost every aspect of EU citizens' lives. At the same time, due to its less centralised architecture, smart computing power at the edge, the need for more antennas and increased dependency on software, 5G networks offer more potential entry points for attackers. Therefore, ensuring the security of the EU's future 5G networks is of utmost importance.

While operators are largely responsible for the secure rollout of 5G, and Member States are responsible for national security, network security is an issue of strategic importance for the entire EU. A coordinated approach based on robust security measures at national and EU level will help Europe to remain one of the leading regions in the 5G deployment.

What is the EU toolbox on 5G Cybersecurity about?

The objective of the EU toolbox on 5G Cybersecurity is to setout a coordinated European approach based on a common set of measures, aimed at mitigating the main cybersecurity risks of 5G networks that were identified in the EU coordinated risk assessment report. It also intends to provide guidance in the selection and prioritisation of measures that should be part of national and EU risk mitigation plans. The ultimate goal is to create a robust and objective framework of security measures, which will ensure an adequate level of cybersecurity of 5G networks across the EU, through coordinated approaches among Member States. The approach taken fully respects the openness of the EU single market, is a risk-based one and solely on security grounds.

Which are the main conclusions of the toolbox?

The toolbox recommends a set of key actions for the Member States and/or the Commission.

Member States agreed to ensure that they have measures in place (including relevant powers for national authorities) to respond appropriately and proportionately to the risks already identified as well as possible future risks. In particular, they agreed to ensure that they would be able to restrict, prohibit, and/or impose specific requirements and conditions, in accordance with a risk-based approach, for the supply, deployment, and operation of 5G network equipment. In particular, they should:

- **Strengthen security requirements for mobile network operators** (e.g. strict access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.);
- Assess the risk profile of suppliers; as a consequence, **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-wide coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions);
- 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 an adequate balance of suppliers at national level and **avoid dependency on suppliers considered to be high risk**; this also requires avoiding any situations of lock-in with a single supplier, including by promoting greater interoperability of equipment;

The toolbox recommends that the Commission, together with Member States, should contribute to:

- Maintaining a **diverse and sustainable 5G supply chain** in order to avoid long-term dependency, including by:

o Making full use of the existing EU tools and instruments, in particular through the screening of foreign direct investments (FDI) affecting 5G key assets and by avoiding distortions in the 5G supply market stemming from potential dumping or subsidies; and

o Further strengthening **EU capacities in the 5G and post-5G technologies**, by using relevant EU programmes and funding.

- Facilitating coordination between Member states regarding **standardisation** to achieve specific security objectives **and developing relevant EU-wide certification scheme(s)** in order to promote more secure products and processes.

What is the state of implementation of the 5G security toolbox in Member States?*

- On 24 July 2020, EU Member States, with the support of the Commission and ENISA, the EU Agency for Cybersecurity, published a report on the progress made in implementing the joint EU toolbox of mitigating measures, which was agreed by the Member States and endorsed by a Commission Communication in January 2020.

- According to the report, good progress has already been achievedfor some of the toolbox measures, notably in the following areas:

o The **powers of national regulatory authorities to regulate 5G security**, have been or are in the process of being reinforced in a large majority of Member States, including powers to regulate the procurement of network equipment and services by operators.

o Measures aimed at **restricting the involvement of suppliers based on their risk profile** are already in place in a few Member States and at an advanced stage of preparation in many others. The report calls on other Member States to further advance and complete this process in the coming months. With regards to the precise scope of these restrictions, the report highlights the importance to look at the network as a whole and address core network elements as well as other critical and highly sensitive elements, including management functions and the radio access network, and of imposing restrictions also on other key assets, such asdefined geographical areas, government or other critical entities.

o **Network security and resilience requirements for mobile operators** are being reviewed in a majority of Member states. The report stresses the importance to ensure that these requirements are strengthened, that they follow the latest state-of-the-art practices and that their implementation by operators is effectively audited and enforced.

- On the other hand, some measures are at a less advanced stage of implementation. In particular according to the report:

o Progress is urgently needed to mitigate the **risk of dependency on high-risk suppliers,** also with a view to reducing dependencies at Union level. This should be based on a thorough inventory of the networks' supply chain and implies monitoring the evolution of the situation.

o Challenges have been identified in **designing and imposing appropriate multi-vendor strategies for individual operators or at national level** due to technical or operational difficulties (e.g. lack of interoperability, size of the country, etc.).

o As regards the **screening of Foreign Direct Investments**, steps should be taken to introduce national FDI screening mechanism without delay in 13 Member States where it is not yet in place, including in view of the approaching application of the EU investment screening framework as of October 2020. These screening mechanisms should be applied to investment developments potentially affecting the 5G value chain, taking into account the objectives of the toolbox.

What should national authorities do to move forward in implementing the toolbox?*

- **Complete the implementation process** at national level, while paying **particular attention to elements** highlighted in the progress report;

- **Exchange more information about challenges, best practices and solutions** for implementing the toolbox measures;

- Continue **monitoring and evaluating the implementation of the toolbox**;

- Continue working with the Commission to implement EU-level actions listed in the toolbox, including in the area of **standardisation and certification**, trade defence instruments and competition rules to avoid distortions in the 5G supply market.

- Also, **investing in EU capacities** in the 5G and post-5G technologies, and ensuring 5G projects supported with public funding take into account cybersecurity risks.

What are the different types of measures identified in the EU toolbox?

For each of the nine risk areas identified in the EU coordinated risk assessment report, the toolbox identifies and provides risk mitigation plans. They consist of possible combinations of strategic and technical measures.

- **Strategic measures** identified in the toolbox range from measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities (e.g. risk of interference by non-EU state or state-backed actors), to assessing the risk profile of suppliers and promoting initiatives to support the development of sustainable and diverse 5G suppliers.
- **Technical measures** identified in the toolbox range from ensuring strict access control and secure network management, operation and monitoring to using certification for 5G network components and/or processes.
- **Supporting actions** cover actions in the area of 5G standards, reinforcing testing and auditing capabilities, improving the coordination efforts in case of incidents, or making sure that cybersecurity risks are fully taken into account in EU-funded 5G projects. These supporting actions can enable, assist and enhance the effectiveness of the strategic and technical measures.

What is a risk mitigation plan?

For each of the nine risk areas identified in the EU coordinated risk assessment report, the toolbox identifies and provides risk mitigation plans. They consist of possible combinations of strategic/and or technical measures (together with the appropriate supporting actions) intended to mitigate a security risk.

Are the toolbox measures mandatory?

The EU toolbox on 5G cybersecurity is a document prepared and agreed by the NIS Cooperation Group, which consists of representatives of all Member States authorities, the Commission and the EU Cybersecurity Agency. The development of a coordinated EU approach on 5G cybersecurity relies on the strong commitment by both Member States and the Commission to use and fully implement a key set of recommended measures. The toolbox sets out a precise and objective methodology to address the risks identified in the European risk assessment published in October 2019, while respecting national competences in this area.

At the same time, the roll-out andoperation of 5G networks is a matter of national security. Member States can go further than what is proposed in the toolbox where they identify a need to do so.

How will the EU toolbox be implemented?

An appropriate combination of various types of measures is needed to effectively mitigate the identified risks. Indeed, Member States will need to take a range of mitigation actions to effectively address the security risks related to 5G networks. Measures may be implemented through national and/or EU actions, depending on the specific measure and actions. Some measures may be directly introduced or reinforced at national level, while others may require further or joint action at EU level, in line with the respective national and EU competences.

Does the toolbox address the risk of interference from a third country?

The toolbox addresses all risks identified in the EU coordinated risk assessment, including risks related to the interference from a third country via the 5G supply chain. It does not target any supplier or country in particular. To mitigate this particular risk, the toolbox recommends that all Member States take the following steps:

(1) assess the risk profile of suppliers, having regard to criteria set out in the EU-wide coordinated risk assessment;

(2) as a consequence, 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 (e.g. core network functions, network management and orchestration functions, and access network functions).

How does the Commission Communication complement the EU toolbox?

The Commission Communication endorses the EU toolbox and proposes a way forward for its implementation.Moreover, the Commission will act, as requested in the toolbox, using, where appropriate, all the tools at its disposal to ensure the security of the 5G infrastructure and supply chain, including:

- Telecoms and cybersecurity rules, e.g. support under electronic communications rules, including consideration of implementing acts on technical and organisational security measures;
- Coordination on standardisation, e.g. regarding participation in standardisation bodies, and promoting interoperability though open interfaces
- EU-wide certification, under the EU Cybersecurity Act;
- foreign direct investment screening to protect the European 5G supply chain;
- trade defence instruments: market monitoring and action to protect EU actors in 5G market against potential trade distorting practices (dumping or subsidisation);
- competition rules: market monitoring to ensure competitive outcomes, including in relation to potential lock-in situations;
- public procurement, ensuring that due consideration is given to security aspects when awarding public contracts, as well as through EU funding programmes, and ensuring that beneficiaries comply with relevant security requirements.
- Making full use of incident response and crisis management frameworks at EU level, in response to large-scale cybersecurity incidents.
- Increase investments in research innovation and deployment technologies

What instruments are available at EU level to protect 5G networks?

The EU already has a range of instruments to protect electronic communications networks:

Under the **EU telecommunications framework**, obligations can be imposed on telecommunication operators. Member States are required to ensure the integrity and security of public communications networks and that public communications networks or services take measures to manage security risks. The framework also provides that competent national regulatory authorities have powers to issue binding instructions and ensure compliance.

The **European Electronic Communications Code** that will replace the current framework as of 21 December 2020 maintains and extends the security provisions of the current framework and introduces definitions on the security of networks and services and security incidents. In addition to this, the EECC provides that security measures should take into account all the relevant aspects of certain elements in areas such as security of networks and facilities, handling of security incidents, business continuity management, monitoring, auditing and testing as well as compliance with international standards.

The **NIS Directive** requires operators of essential services in other fields (energy, finance, healthcare, transport, digital service providers, etc.) to take appropriate security measures and to notify serious incidents to the relevant national authority. The NIS Directive also foresees coordination between Member States in case of cross-border incidents affecting operators in its scope. The Commission Work Programme adopted today announces the review of the Directive before the end of 2020.

The **Cybersecurity Act**, which entered into force in June 2019, creates a framework for European cybersecurity certification schemes for products, processes and services. Once in place, certification schemes will also enable producers to demonstrate that they have included specific security features in the early stages of products' design and allow users to ascertain the level of security assurance, on an EU-wide basis. The framework provides an essential supporting tool to promote consistent levels of security. It allows for the development of cybersecurity certification schemes to respond to the needs of users of 5G-related equipment and software.

Furthermore, the Commission will support the implementation of the EU toolbox and will act, as requested by Member States, using all the tools at its disposal to ensure the security of the 5G infrastructure and supply chain, where appropriate (see previous question).

What are the next steps?

As recommended by the NIS Cooperation and supported by the Commission Communication, work will continue within the NIS Cooperation Group to monitor the implementation of the toolbox and to ensure

its effective and consistent application.

The Group will also promote the alignment of national approaches, through further exchanges of experiences, and by working with the Body of European Regulators for Electronic Communications (BEREC).

As part of the implementation of the Commission Recommendation adopted last year, Member States, in cooperation with the Commission, should assess the effects of the Recommendation and determine whether there is need for further action **by 1 October 2020**.

This assessment should take into account the outcome of the EU coordinated risk assessment that was published in October 2019 as well of the effectiveness of the toolbox measures.

*updated 24/07/2020

QANDA/20/127

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email