European Commission

EU TOOLBOX FOR 5G SECURITY

A SET OF ROBUST AND COMPREHENSIVE MEASURES FOR AN EU COORDINATED APPROACH TO SECURE 5G NETWORKS

March 2021
#Cybersecurity

5G: a new technology

While 3G made mobile internet possible and 4G allowed mobile broadband, 5G is expected to become the connectivity infrastructure that will pave the way for new products and services and affect all sectors of society. Benefits will include the following.

E-HEALTH

- Remote health monitoring, patients' records and smart diagnosis
- Utilising robots to help surgeons and improve medical outcomes

SMART ENERGY GRIDS

- Highly efficient power lines and fewer outages on a smaller scale
- Easier deployments with a lower environmental impact

FACTORIES OF THE FUTURE

- Better control over time-sensitive internal processes
- Remote control access to warehouse machinery

MEDIA & ENTERTAINMENT

- An amplified viewing experience, such as virtual reality
- Ultra fast high-bandwidth applications such as video streaming

MOBILITY

- Enabling connected and automated mobility with the goal of zero accidents
- Enabling connectivity in all modes of transport

Europe is the most advanced region in the deployment of large-scale 5G trials in vertical industries (in which close to €1 billion had been invested by the end of 2020), including for 5G transport corridors. By the end of 2020, 5G services were available in 500 European cities.

Cybersecurity of 5G: an imperative precondition

5G networks are the future backbone of our increasingly digitalised economies and societies. Billions of connected objects and systems are concerned, including those used in critical sectors such as energy, transport, banking and health, as well as those used in industrial control systems that carry sensitive information and that support safety systems. Ensuring the cybersecurity and resilience of 5G networks is therefore essential.

At the same time, due to a 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.

Timeline of the EU 5G cybersecurity policy

22 March 2019

Conclusions by the **European Council**.

26 March 2019

The **European Commission** published a **recommendation** for Member States to take concrete actions to assess the cybersecurity risks of 5G networks and to strengthen risk mitigation measures.

9 October 2019

The Member States finalised the **EU coordinated risk assessment** of 5G network security.

21 November 2019

The EU Agency for Cybersecurity published an extensive **report on threats** relating to 5G networks.

29 January 2020

Publication of the **toolbox of mitigation measures** by Member States. Commission communication on implementing the EU toolbox (COM(2020) 50 final of 29 January 2020).

July 2020

Progress report on toolbox implementation.

October 2020

The **European Council** called on the EU and the Member States 'to make full use of the 5G cybersecurity toolbox' and 'to apply the relevant restrictions on high-risk suppliers for key assets'.

December 2020

New EU cybersecurity strategy and **report** on the impacts of the Commission recommendation on 5G cybersecurity.

By June 2021

Commission calls on Member States to **complete the implementation of the main toolbox measures**.

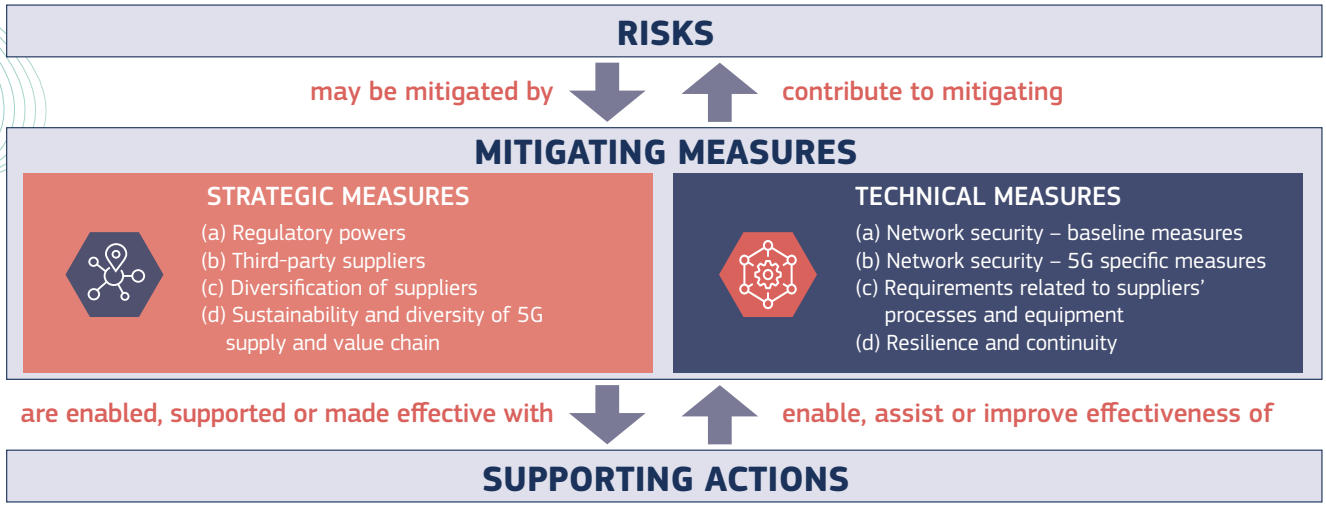
EU risk assessment: risk scenarios

The EU coordinated risk assessment of 5G network security identifies nine main risks grouped into five risk scenarios.

I Risk scenarios related to insufficient security measures	R1 Misconfiguration of networks R2 Lack of access controls
II Risk scenarios related to 5G supply chain	R3 Low product quality R4 Dependency on any single supplier within individual networks or lack of diversity on nationwide basis
III Risk scenarios related to modus operandi of main threat actors	R5 State interference through 5G supply chain R6 Organised crime group exploitation of 5G networks or targeting of end users
IV Risk scenarios related to interdependencies between 5G networks and other critical systems	R7 Significant disruption of critical infrastructures or services R8 Massive failure of networks due to interruption of electricity supply or other support systems
V Risk scenarios related to end-user devices	R9 Exploitation of the internet of things, handsets or smart devices

EU toolbox for 5G security

Based on the EU coordinated risk assessment of 5G network security, the toolbox lays out a range of security measures aiming to mitigate risks effectively and ensure secure 5G networks are deployed across Europe. It sets out detailed **mitigation plans** for each of the identified risks and recommends a set of **key strategic and technical measures** which should be taken by all Member States and/or by the Commission.



EU toolbox conclusions: key measures

Member States should have measures in place and powers to mitigate risks. In particular they should:

- strengthen **security requirements** for **mobile network operators**;
- assess the risk profile of suppliers; apply relevant **restrictions for suppliers considered as high risk**, including necessary exclusions for key assets;
- ensure that each operator has an appropriate **multi-vendor strategy** to **avoid** or **limit** any **major dependency** on a single supplier and avoid dependency on suppliers considered to be high risk.

The **European Commission**, together with Member States, should take measures to:

- maintain a **diverse** and **sustainable 5G supply chain** in order to avoid long-term dependency, including by:
  - making full use of the existing EU tools and instruments (foreign and direct investment screening, trade defence instruments, competition),
  - further strengthening EU capacities in the 5G and post-5G technologies by using relevant EU programmes and funding;
- facilitate coordination between Member States regarding **standardisation** to achieve specific security objectives and develop relevant EU-wide **certification schemes**.

In addition, the mandate of the **Network and Information Systems Cooperation Group work stream** should be extended to support, monitor and evaluate the implementation of the toolbox.

Risk mitigation plans: examples of toolbox measures

For each of the nine risk areas identified in the EU coordinated risk assessment report, the toolbox identifies risk mitigation plans. They consist of possible combinations of measures based on their effectiveness.

The toolbox provides guidance on objective criteria, including technical and non-technical risk factors, to assess the risk profile of suppliers, i.e. risk of interference by a non-EU country; ability to supply and cybersecurity practices.

SM03	**Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks – for key assets**	- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment and adding country-specific information (e.g. threat assessment from national security services), for national competent authorities and mobile network operators (MNOs) to: – perform rigorous assessments of the risk profiles of all relevant suppliers at national level and/or EU level (for example jointly with other Member States or other MNOs); – based on the risk profile assessment, apply restrictions – including necessary exclusions to effectively mitigate risks – for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions and access network functions); – take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management and/or specific requirements for suppliers based on their risk profiles.

The toolbox provides guidance on the sensitivity of network elements and functions.

TM03	**Ensuring strict access controls**	Ensure that MNOs implement adequate, flexible and verifiable technical measures to ensure that: – strict network access controls are applied; – the principle of least privilege is applied, ensuring that various rights in the network (e.g. access rights between network functions, network administrators' rights, virtualisation configuration) are minimised; – the segregation of duties principle is applied; – procedures are in place to ensure that these rules are in effect all the time and evolve with the network. In setting the access control policies, particular care should be taken to ensure that remote access by third parties, especially suppliers considered to be high risk, is minimised and/or avoided whenever possible. When remote access is necessary, for example to address service outages, the MNO should apply appropriate authentication, authorisation, logging and auditing so as to have clear visibility on access to data and configuration changes or network alterations.

Next steps (under the EU cybersecurity strategy for the digital decade)

- Complete the implementation of the main toolbox measures by the second quarter of 2021.
- Ensure that the identified risks have been mitigated adequately and in a coordinated way, in particular as regards the objective of minimising exposure to high-risk suppliers and of avoiding dependency on these suppliers at national and EU levels.
- Continue and deepen coordination at EU level, focusing on key objectives:

1. Ensuring convergent national approaches for effective risk mitigation across the EU

2. Supporting continuous exchange of knowledge and capacity building

3. Promoting supply-chain resilience, and other EU strategic security objectives

Publications Office of the European Union

PDF ISBN 978-92-76-37717-7 doi:10.2759/048142 KK-02-21-626-EN-N
PRINT ISBN 978-92-76-37743-6 doi:10.2759/500089 KK-02-21-626-EN-C

Updated 2021-05-25