5G CYBERSECURITY

Review of the impacts of the Commission Recommendation and areas for further action

European Commission

MAIN STEPS

26 March 2019 - Commission **Recommendation** on the cybersecurity of 5G networks

July 2019 - Member States national risk assessments

9 October 2019 - EU coordinated risk assessment of 5G networks security by NIS Cooperation Group

29 January 2020 - EU **Toolbox of mitigation measures** and Commission Communication on the implementation of the EU Toolbox

24 July 2020 - Progress report on Toolbox implementation by NIS Cooperation Group

16 December 2020 - Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks

TOOLBOX STRUCTURE AND METHODOLOGY

**EU Toolbox measures aimed at addressing
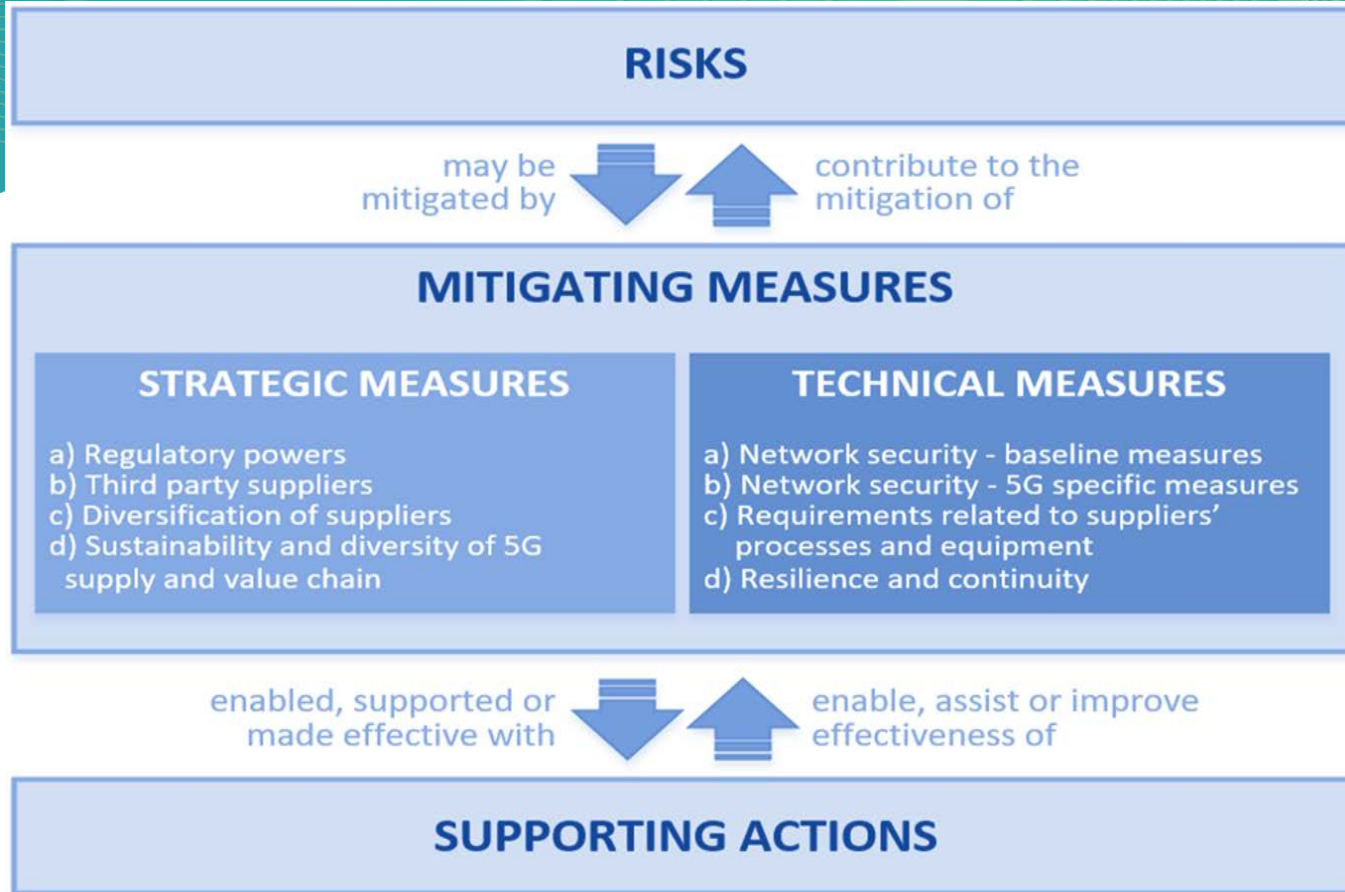9 risks categories in EU Coordinated risk assessment**

Three levels:

1.
Comprehensive list of relevant **MEASURES** and supporting ACTIONS

2.
Risk MITIGATION PLANS: highest effectiveness measures for each risk

3.
Toolbox conclusions: **KEY MEASURES TO BE TAKEN BY ALL MS and/or COM**

EU TOOLBOX- MEASURES (level 1)

RISKS

may be mitigated by ⬇ ⬆ contribute to the mitigation of

MITIGATING MEASURES

STRATEGIC MEASURES

a) Regulatory powers
b) Third party suppliers
c) Diversification of suppliers
d) Sustainability and diversity of 5G supply and value chain

TECHNICAL MEASURES

a) Network security - baseline measures
b) Network security - 5G specific measures
c) Requirements related to suppliers' processes and equipment
d) Resilience and continuity

enabled, supported or made effective with ⬇ ⬆ enable, assist or improve effectiveness of

SUPPORTING ACTIONS

Identifies **8 strategic and 11 technical measures** to mitigate the risks, and 10 corresponding supporting actions to reinforce their effectiveness.

EU TOOLBOX- MITIGATION PLANS (level 2)

Provides **risk mitigation plans** for all 9 risk categories identified in the EU risk assessment

EU TOOLBOX – CONCLUSIONS (1/2) (level 3)

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

strengthen **security requirements** for mobile network operators;

assess the **risk profile of suppliers**; as a consequence, **apply relevant restrictions/ exclusions for high-risk suppliers**;

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**.

EU TOOLBOX – CONCLUSIONS (2/2)

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**;
  - 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 developing relevant EU-wide **certification schemes.**

MAIN ELEMENTS OF THE REVIEW

The review should '*assess the impacts of the Recommendation 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.*'

1. Achievements: **Report on the Impacts of the Commission Recommendation of March 2019**

2. Next steps: **EU's Cybersecurity Strategy for the Digital Decade (vision, key objectives and actions)**

MAIN INPUTS FOR THE REVIEW

- ✓ **Progress report by NIS Cooperation Group (July 2020)**

- ✓ **Thematic meetings in NIS Work Stream** on strategic and technical measures

- ✓ **BEREC survey** on vendor diversity

- ✓ '**Country meetings**' with each Member State organised by the Commission and ENISA over the autumn

- ✓ **Other activities** (EU level actions, ENISA work, etc.)

IMPACTS (1) - MEMBER STATES' VIEWS

Overall approach

- Common EU vision
- Timely process, national and EU momentum
- Collaborative approach suitable for complex issue
- Allowed to build and pool knowledge and expertise
- Flexibility , respecting national competences

Toolbox process

- Objective, risk-based and proportionate approach
- National situational analysis and comprehensive / common understanding of risks
- Coordinated approach to risk mitigation

Challenges

- Ambitious timelines
- Further alignment of national approaches
- Evolving technology
- Limited resources
- External dimension: need to take into account developments

IMPACTS (2) - TOOLBOX IMPLEMENTATION

- **All Member States have made further progress** in implementing the various measures at national level, with a very large majority indicating clear plans and timelines.

- Most Member States estimate that they will complete the implementation of the main Toolbox measures **by mid-2021**.

- Differences in the state of play regarding individual measures: some Member States **more advanced in certain areas than in others**.

- Areas where more efforts and particular attention is needed, the assessment and **conclusions of the Progress report remain entirely valid**.

- Many Member States intend to keep a structured process to adjust measures and reflect future needs and evolutions.

IMPACTS (3) - EU LEVEL ACTIONS

Certification and standardisation
- Discussion on certification scheme for 5G
- Other schemes (non 5G-specific)
- Standardisation: ENISA report

EU capacities
- R&I investments and other programmes

EU funding/ conditions
- Inclusion of relevant security conditions in relevant programmes

International
- Activities to present the Toolbox approach

NEXT STEPS (1) - NEW CYBERSECURITY STRATEGY

- 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 the exposure to high risk suppliers** and of **avoiding dependency on these suppliers** at national and at Union level.

- **Continue and deepen coordination** at EU level, focusing on key objectives

NEXT STEPS (2) - KEY OBJECTIVES

3 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

Key objective 1: Ensuring convergent national approaches for effective risk mitigation across the EU

Areas	Main short- and mid-term actions	Lead actors
Toolbox implementation by Member States	Complete the implementation of the measures recommended in the Toolbox conclusions by the second quarter of 2021, with periodic stocktaking within the NIS Work Stream.	Member States authorities
Exchange of information and best practices on strategic measures related to suppliers	Intensify exchanges of information and consider possible best practices, in particular about: • Restrictions on high-risk suppliers (SM03) and measures related to the provision of managed services (SM04); • Supply chain security and resilience, notably following up on the survey conducted by BEREC about SM05-SM06.	Member States authorities, Commission
Capacity building and guidance on technical measures	Conduct technical deep-dives and develop common guidance and tools, including: • A comprehensive and dynamic matrix of security controls and best practices for 5G security; • Guidance in support of implementation of selected technical measures from the Toolbox.	ENISA, Member States authorities

Key objective 2: Supporting continuous exchange of knowledge and capacity building

Areas	Main short- and mid-term actions	Lead actors
Continuous knowledge building	Organise knowledge building activities on technology and related challenges (open architectures, 5G features – e.g. virtualisation, containerisation, slicing etc.), threat landscape evolutions, real-life incidents, etc.	ENISA, Member states authorities, other stakeholders
Risk assessments	Update and exchange information on updated national risk assessments	Member States authorities, Commission, ENISA
Joint EU-funded projects to support the Toolbox implementation	Provide financial support to projects supporting the Toolbox implementation using EU funding, notably under the Digital Europe Programme (e.g. capacity building projects for national authorities, test beds or other advanced capacities, etc.)	Member States authorities, Commission
Cooperation among stakeholders	Foster collaboration and cooperation between national authorities engaged in 5G cybersecurity (e.g. NIS Cooperation Group, cybersecurity authorities, telecom regulatory authorities) and with private stakeholders	Member States authorities, Commission, ENISA

Key objective 3: Promote supply chain resilience, and other EU strategic security objectives

Areas	Main short- and mid-term actions	Lead actors
Standardisation	Define and implement a concrete action plan to enhance EU representation in standard setting bodies as part of the next steps of the work of the NIS sub-group on standardisation, in order to achieve specific security objectives, including the promotion of interoperable interfaces to facilitate diversification of suppliers.	Member States authorities
Supply chain resilience	• Conduct an in-depth analysis of the 5G ecosystem and supply chain to better identify and monitor key assets and potential critical dependencies • Ensure the functioning of the 5G market and supply chain is in line with EU trade and competition rules and objectives, as defined in the Commission Communication of 29 January, and that FDI screening is applied to investment developments potentially affecting the 5G value chain, taking into account the objectives of the Toolbox. • Monitor existing and expected market trends and assess the risks and opportunities in the field of Open RAN, notably through an independent study	Member States authorities, Commission
Certification	Initiate preparations of relevant candidate certification scheme(s) for key 5G components and suppliers' processes, to help address certain risks related to technical vulnerabilities, as defined in the Toolbox risk mitigation plans.	Commission, ENISA, national authorities, other stakeholders
EU capacities and secure network roll-outs	• Invest into R&I and capacities, notably through the adoption of the Smart Networks and Services Partnership. • Implement relevant security conditions for EU funding programmes and financial instruments (internal and external), as announced in the Commission Communication of 29 January.	Member States, Commission, 5G industry stakeholders
External aspects	Respond favourably to third country requests who would like to understand and potentially use the Toolbox approach developed by the EU.	Member States, Commission, External Action Service

THANK YOU

European Commission