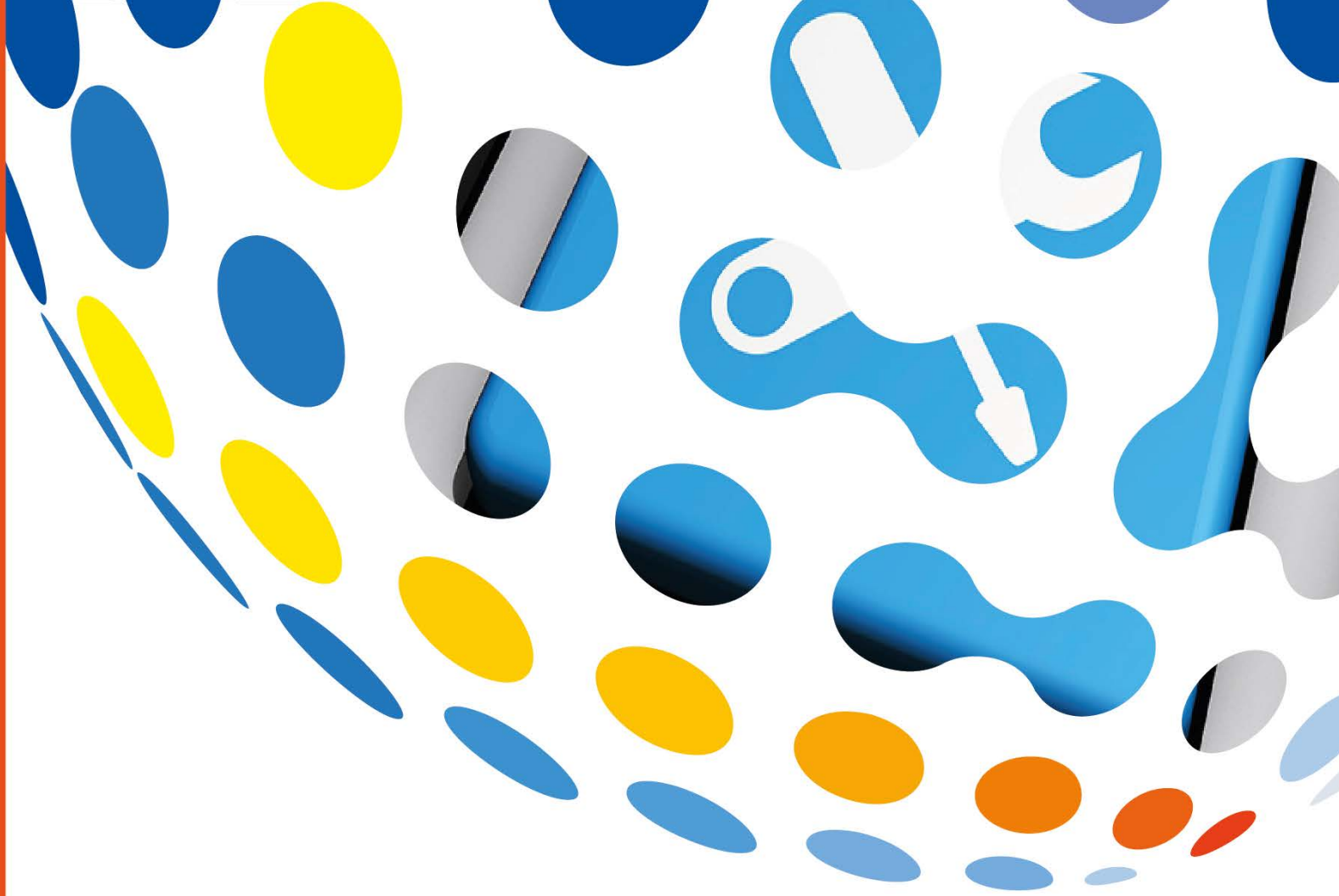


Cybersecurity of 5G networks EU Toolbox of risk mitigating measures

CG Publication

01/2020

NIS COOPERATION GROUP

Table of content

1. Introduction

5G networks will play a central role in achieving the digital transformation of the EU's economy and society. Indeed, 5G networks have the potential to enable and support a wide range of applications and functions, extending far beyond the provision of mobile communication services between end-users. With worldwide 5G revenues to reach an estimated €225 billion in 2025[1], 5G technologies and services are a key asset for Europe to be able to compete in the global market.

The cybersecurity of 5G networks is therefore essential to protect our economies and societies and to enable the full potential of the important opportunities they will bring. It is also crucial for ensuring the technological sovereignty of the Union.

Following the support expressed by the European Council on 22 March, 2019 for a concerted approach to the security of 5G networks, the European Commission adopted its Recommendation on the cybersecurity of 5G networks (hereafter 'The Recommendation') on 26 March, 2019. The Recommendation called on Member States to complete national risk assessments and review national measures, to work together at EU level on a coordinated risk assessment and to prepare a toolbox of possible mitigating measures.

Each Member State completed its own national risk assessment of its 5G network infrastructures and transmitted the results to the Commission and ENISA - the European Union Agency for Cybersecurity.

Based on these national risk assessments, on 9 October, 2019 Member States - with the support of ENISA and the Commission - published a report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks[2]. This report identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities, such as the legal and policy framework to which suppliers of information and communications technologies equipment may be subject to in third countries), and the main associated risks. To complement this report and as a further input for the toolbox, ENISA carried out a dedicated threat landscape mapping[3], consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting these.

The Council Conclusions of 3 December, 2019 endorsed the work of the Member States' Cooperation Group on Network and Information Security (NIS Cooperation Group), supporting the findings of the coordinated risk assessment. In particular, the Council welcomed 'the ongoing joint European efforts on safeguarding the security of 5G networks based in particular on the Commission Recommendation on Cyber Security of 5G Networks' and stressed 'the importance of a coordinated approach and effective implementation of the Recommendation in order to avoid fragmentation in the Single Market'. To this effect, the Council called upon Member States, the Commission and ENISA, to 'take all necessary measures within their competences to ensure the security and integrity of electronic communication networks, in particular 5G networks and to continue to consolidate a coordinated approach to address the security challenges related to 5G technologies.' [4]

[1] ABI Research projection: https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue.
[2] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.
[3] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.
[4] Council Conclusions on the significance of 5G to the European economy and the need to mitigate security risks linked to 5G 3 December, 2019 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf .

The EU coordinated risk assessment report highlights a number of important security challenges which are likely to appear or become more prominent in 5G networks. These security challenges are mainly linked to:

- Increasing security concerns related to the availability and integrity of the networks, in addition to the confidentiality and privacy concerns;

- Key innovations in the 5G technology (which will also bring a number of specific security improvements), in particular the increased important role of software and the wide range of services and applications enabled by 5G networks; and

- The role of suppliers in building and operating 5G networks, the complexity of the interlinkages between suppliers and operators, and the degree of dependency on individual suppliers.

The report further concludes that these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem, and making it essential for Member States to take the necessary mitigating measures.

The EU coordinated risk assessment report provides the basis to identify mitigation measures that can be applied at national and European level.

2. Objectives of the toolbox

The objectives of this toolbox are to identify a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks, as they have been identified in the EU coordinated risk assessment report, and to provide guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level. It does this in order to create a robust framework of measures with a view to ensure an adequate level of cybersecurity of 5G networks across the EU and coordinated approaches among Member States.

The EU coordinated risk assessment identifies a number of categories of risks of strategic importance from an EU perspective illustrated by concrete risk scenarios. These reflect relevant combinations of vulnerabilities, threats and threat actors and the identified assets.

Table 1 - Risk categories and scenarios

(source: the EU coordinated risk assessment report)

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 nation-wide basis
III - Risk scenarios related to *modus operandi* of main threat actors	**R5-** State interference through 5G supply chain **R6-** Exploitation of 5G networks by organised crime or organised crime group targeting 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 IoT (Internet of Things), handsets or smart devices

To effectively address these risks and strengthen the security and resilience of 5G networks a comprehensive approach is required. This implies putting in place a key set of measures, as well as related supporting actions which can simultaneously address the risks. Ultimately, the key to ensure coordinated Member State approaches will be the effective implementation of the risk mitigation measures and actions in all Member States, as adapted to the respective situation in each Member State.

This toolbox also provides an indicative assessment of measures which would require or benefit from a common approach and/or some form of coordination at EU level, or which may be best implemented in coordination with other Member States or by individual Member States, depending on the respective national context.

Altogether, the measures presented in this toolbox contribute to achieving a number of important and mutually reinforcing security objectives, which are relevant to address the risks identified in the risk assessment report and protect the confidentiality, integrity and availability of 5G networks:

- Reinforcing security in the design, deployment and operation of networks;
- Raising baseline security standards for the security of product and services;
- Minimising the exposure to risks stemming from the risk profile of individual suppliers;
- Avoiding or limiting major dependencies on any single supplier in 5G networks; and
- Promoting a diverse, competitive and sustainable market for 5G equipment, including by maintaining EU capacities in the 5G value chain.

The measures identified are presented in *Section 4* of this report and further detailed in the annexed tables.

3. Existing frameworks and measures

This section aims at mapping and describing the relevant existing regulatory frameworks and instruments as well as the baseline of measures and mitigations already in place, in order to take them into account when establishing risk mitigation plans, and possibly also when introducing new measures.

3.1. EU level instruments

3.1.1 Main Union regulatory frameworks

The EU uses a range of instruments to protect electronic communications networks, including the EU telecommunications framework[5], the NIS Directive (Directive on Security of Network & Information Systems)[6] and the Cybersecurity Act[7][8].

Under the EU telecommunications framework, obligations can be imposed on telecommunication operators by the respective Member State(s) in which they are providing service. Member States are required to ensure that the integrity and security of public communications networks are maintained and have 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[9]. The framework also provides that competent national regulatory authorities have powers to issue binding instructions and ensure compliance. In addition, under Directive 2002/20/EC[10] Member States are allowed to attach to a general authorisation conditions concerning the security of public networks against unauthorised access, for the purpose of protecting the confidentiality of communications, in accordance with Directive 2002/58/EC[11].

The **European Electronic Communications Code (EECC),** which will replace the current framework as of 21 December 2020, maintains the security provisions of the current framework (in Title V, Articles 40 and 41) and also introduces definitions on the security of networks and services[12]

[5] Directive 2002/21/EC as last amended by Directive 2009/140/EC of 25 November, 2009 on a common regulatory framework for electronic communications networks and services, and Directive 2018/1972 of 11 December, 2018 establishing the European Electronic Communications Code.

[6] Directive (EU) 2016/1148 of 6 July, 2016 concerning measures for a high common level of security of network and information systems across the Union.

[7] Regulation (EU) 2019/881 of 17 April, 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

[8] To support the implementation of these obligations and instruments, the Union has set up a number of cooperation bodies. The main one is the NIS Cooperation Group established by the NIS Directive which brings together competent authorities in order to support and facilitate cooperation, in particular by providing strategic guidance. The CSIRTs Network - as a network of national CSIRTs from EU Member States - facilitates operational information exchange. 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, threats and assets.

[9] Article 13a on the security and integrity of networks and services of Directive 2002/21/EC as last amended by Directive 2009/140/EC; and Articles 40 and 41 of Directive 2018/1972.

[10] Directive 2002/20/EC of 7 March, 2002 on the authorisation of electronic communications networks and services (Authorisation Directive).

[11] Directive 2002/58/EC of 12 July, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[12] Specifically under Article 2, (21), 'security of networks and services' is defined as 'the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or

and security incidents. In addition to this, the EECC provides that security measures should, as a minimum, 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[13].

Neither the current framework nor the EECC include any provisions directly applicable to the network equipment manufacturers and other service providers in the electronic communications supply chain, since these providers do not fall under their scope.

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 **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 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.

3.1.2 Other relevant EU-level instruments:

In the area of trade policy, as of 11 October 2020, the EU's **Foreign Direct Investment (FDI) Screening Regulation**[14] will provide an instrument to coordinate detection and address potential security risks related to foreign direct investments into the EU, amongst others, in sensitive areas such as critical technologies and critical infrastructures. Applied to the 5G toolbox, and in order to protect key 5G assets and avoid dependencies, the FDI screening mechanism can provide an important instrument to regularly and better monitor FDI developments into the EU along the 5G value chain. Should specific FDI developments fall under the scope of the Regulation, then these can be addressed and Member States can undertake the appropriate mitigating actions.

Furthermore, the EU uses **trade defence instruments** to re-establish a competitive environment for the EU industry when injured by dumped or subsided imports. Specifically, the European Commission is responsible for investigating allegations of dumping by exporting producers from non-EU countries, or in the case of trade-distorting subsidies. It usually opens an investigation after

confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services'.

[13] Preamble (94): …'as regards security of networks and facilities: physical and environmental security, security of supply, access control to networks and integrity of networks; as regards handling of security incidents: handling procedures, security incident detection capability, security incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and service testing, security assessments and compliance monitoring; and compliance with international standards.'

[14] Regulation (EU) 2019/452 of 19 March, 2019 establishing a framework for the screening of foreign direct investments into the Union.

receiving a complaint from the EU producers concerned, but it could also exceptionally do so on its own initiative[15].

In accordance with existing rules on **public procurement**[16,] Member States are encouraged to not award contracts solely on the basis of the lowest price, but also to take into account quality in areas such as security, labour and environmental standards. Moreover, they do not prevent Member States from imposing or enforcing measures necessary to protect public security or essential security interests. Tenders from bidders that do not have secured access to the EU procurement market (based on binding international or bilateral free trade agreements covering public procurement) may also be excluded. Member States may also under certain conditions exclude an economic operator that could cause a risk to the essential national security interests. Furthermore, within the field of defence and security, public buyers do not have to give access to the tenders to third country operators.

Maintaining and further developing European capacities in the area of 5G and in particular in critical parts of the value chain by leveraging **EU Research & Innovation Funding programmes and Industrial policy** tools is a strategic risk mitigating measure addressing the risk of dependencies. By supporting disruptive and ambitious research, innovation and deployment funding programmes, such as Horizon Europe, Digital Europe Programme, and the Connecting Europe Facility (CEF) can facilitate the emergence of European competitive sourcing options, especially as regards to processors and critical software. The funding programmes also contain security-related provisions.

Moreover, linked to the EU's state aid regime, **IPCEIs (Important Projects of Common European Interest)** make it possible to bring together knowledge, expertise, financial resources and economic actors throughout the Union[17,] so as to overcome important market or systemic failures and societal challenges which cannot otherwise be addressed. They are designed to bring together public and private sectors to undertake large-scale projects that provide significant benefits to the Union and its citizens.

Finally, **other relevant or potentially relevant tools and frameworks at EU and national** level include data protection and privacy rules (in particular the General Data Protection Regulation and e-Privacy Directive)[18,] the Radio Equipment Directive[19,] EU rules on export controls[20], requirements applicable to critical infrastructures, as well as frameworks aimed at responding to cyber incidents

[15] Anti-dumping legal instrument (Regulation (EU) 2016/1036), anti-subsidy legal instrument (Regulation (EU) 2016/1037), safeguards (Regulation (EU) 2015/478).

[16] E.g. Directive 2014/24/EU of 26 February, 2014 on Public Procurement; Directive 2009/81/EC of 13 July, 2009 in the fields of defence and security, C(2019)5494 Guidance of 24 July, 2019 on the participation of 3rd country bidders and goods in the EU procurement market.

[17] Based on Article 107(3)(b) of the Treaty on the Functioning of the European Union (TFEU) and C (2014) 188/02 on the criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interests.

[18] Regulation (EU) 2016/679 on protection of natural persons with regard to the processing of personal data and on the free movement of such data; Dir. 2002/58/EC on the processing of personal data & the protection of privacy in the electronic communications sector.

[19] Directive 2014/53/EU of 16 April, 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment.

[20] Regulation EC 428 2009 of 5 May, 2009 on a Community regime for the control of exports, transfer, brokering and transit of dual-use goods, and COM (2016) 616 proposal of 28 September,2016

or crisis, in particular the Blueprint for a coordinated response to large-scale cybersecurity incidents and crisis and the Cyber Diplomacy toolbox[21].

3.2. National implementation of EU telecoms rules

Under the current EU telecom rules[22], EU Member States supervise a set of security requirements for telecom providers. As described under 3.1.1 above, Article 13a requires Member States to ensure that:

- Telecom providers assess risks and take appropriate security measures;
- Telecom providers take resilience measures to mitigate disruptions of their networks and/or services; and
- Telecom providers notify significant incidents to the relevant national authorities.

Most national laws transposing the current EU legal framework were adopted around 2011. In terms of supervision method and obligations, Member States have followed diverse approaches. For instance, where binding rules apply to mobile network operators, they may cover different types of technical and organisational measures. In Member States where security measures are further clarified in more technical and practical detail (often via secondary legislation), they often refer to the security measures of the Article 13a security framework[23].

At this stage, with very few exceptions, national measures in this area do not explicitly provide for advanced security requirements specifically relating to the roll-out of 5G networks. Similarly, they do not explicitly provide for ex-ante regulatory powers or obligations related to security in the context of procurement and deployment by operators of network equipment, nor do they include provisions aimed at promoting security and resilience through an appropriate degree of supplier diversity or at addressing risks and vulnerabilities related to the risk profile of individual suppliers.

[21] Framework for a Joint EU Diplomatic response to malicious cyber activities (Council Conclusions 20 November, 2017, 9916/17) and Commission Recommendation (Blueprint) on a coordinated response to large-scale cybersecurity incidents & crisis (EU 2017/1584). A Work Stream within the NIS Cooperation Group has undertaken the task of implementing the operational layer provided for by the Blueprint.

[22] Directive 2002/21/EC as last amended by Directive 2009/140/EC on a common regulatory framework for electronic communications networks and services 25.11.2009, and Directive 2018/1972 of 11 December, 2018 establishing the European Electronic Communications Code.

[23] Technical guidance on the security measures in Article 13a (https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures) is a detailed security framework developed jointly by Member States experts to promote a common approach to supervision and/or good practices for the sector security supervision across the EU. The framework covers a wide range of security measures, at a high level and applies to different types of telecom providers.

3.3. Standardisation (baseline work in 3GPP)

5G security issues are increasingly being addressed in the work undertaken by standards bodies, notably within the workgroup on Service and System Aspects 3 (SA3)[24] of the 3rd Generation Partnership Project (3GPP)[25]. Apart from standards, it may also be useful to take into account the security architecture defined by 5G-PPP (based on the deliverables by 5G-Ensure) that, stresses the importance of management domains.

5G technologies and standards could improve security compared to previous generations of mobile networks due to the introduction of several new security-related features, such as stricter authentication processes in the radio interface. These new security features will however not all be activated by default in the network equipment, since some of them are optional for implementation for suppliers or for use by operators. Therefore, the overall effectiveness of these security features will greatly depend upon how the operators deploy and manage their networks.

As indicated in the EU coordinated risk assessment report the SA3 Working Group is also addressing the lawful interception requirements in 5G systems and intends to produce all specifications needed to meet those requirements[26].

4. Measures and mitigation plans

The measures presented in this toolbox are addressed to and for implementation by national and EU responsible authorities and agencies, each with their respective capacities and competences which can range from regulatory oversight to their national security role.

In line with the EU coordinated risk assessment report, the measures concern the relevant security stakeholders in the 5G ecosystem[27], these being primarily **mobile network operators (MNOs)**[28] **and their suppliers, in particular telecom equipment manufacturers.**

On the one hand, mobile network operators have a central, decision-making role, giving them leverage on the overall secure operation of their networks. On the other hand, telecom equipment manufacturers are responsible for the provision of software and hardware required to operate the networks.

The measures presented below and their description build on the relevant findings of the EU coordinated risk assessment report. In particular:

[24] The Service and System Aspects 3 (SA3) Working Group is responsible for security and privacy in 5G standards.

[25] The 3GPP is the main global body for developing standards for mobile communications, a collaboration between seven Organisational Partners, from Europe (ETSI), USA (ATIS), China (CCSA), Japan (ARIB, TTC), Korea (TTA) and India (TSDSI). 3GPP technical specification groups have standardised industry security features in 3G, 4G and now 5G standards.

[26] In its conclusions of 3 December 2019 (14517/19), the Council 'stresses the need to address and mitigate potential challenges arising from the deployment of 5G networks and services to law enforcement including e.g. lawful interception.'

[27] Those stakeholders have been identified in the EU coordinated risk assessment and comprise: Mobile network operators; Suppliers of mobile network operators (including telecom equipment manufacturers and other third-party suppliers, such as cloud infrastructure providers, systems integrators, security and maintenance contractors, transmission equipment manufacturers); Manufacturers of connected devices and related service providers; and Other stakeholders (including service and content providers and end-users of 5G mobile networks).

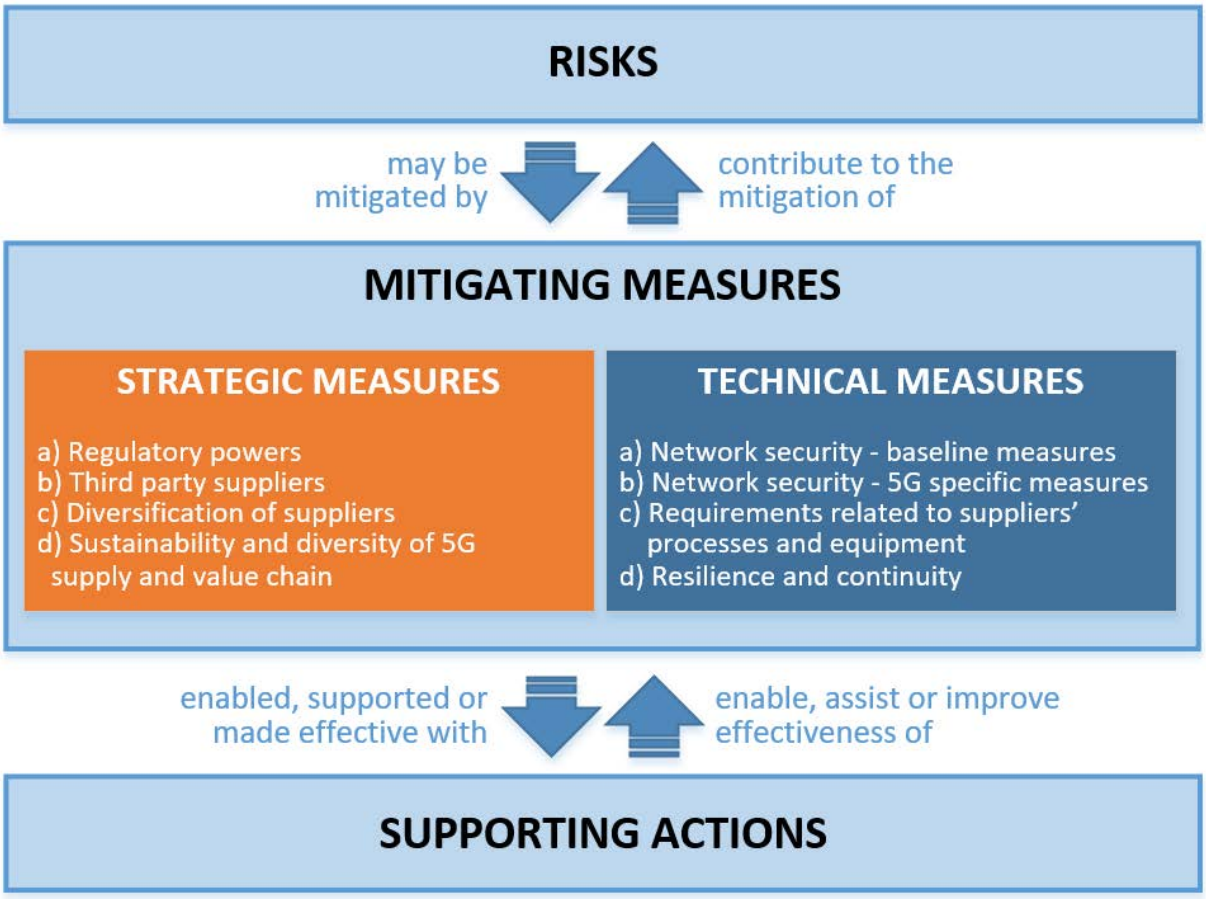
[28] Mobile virtual network operators (MVNOs) and critical infrastructure operators from another sector than telecommunications, which could operate 5G networks for their own activities or on behalf of third parties, would fall under a similar category of stakeholders.

- Where measures refer to **critical or sensitive network component or functions**, the identification of these components or functions should be based on and consistent with the **high-level categorisation of asset sensitivity defined in the EU coordinated risk assessment report** (see annex 2 of this toolbox and paragraph 2.21 of the EU coordinated risk assessment report).

- Where measures refer to the **risk profile of individual suppliers**, the assessment of the risk profile should take into account the **factors defined in the EU coordinated risk assessment**[29] (see annex 2 of this toolbox and para 2.37 of the EU coordinated risk assessment report).

4.1. Measures and supporting actions

Table 2- Toolbox measures and supporting actions



The mitigating measures are grouped into two general categories: **strategic and technical.**

[29] The EU coordinated risk assessment report identifies several risk factors for the assessment of a supplier's risk profile, notably: the likelihood of the supplier being subject to interference from a non-EU country (this may be facilitated by, but not limited to, the presence of certain factors, which are also listed in the EU coordinated risk assessment report); the supplier's ability to assure supply; and the overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

These measures (detailed in annex 1, table 1) can be used to mitigate the **risks** identified in the EU coordinated risk assessment report. They can be complemented by supporting actions to reinforce their effectiveness.

4.1.1 Strategic measures cover 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 a third country or dependency risks), as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic, long-term dependency risks. Strategic measures are potentially highly effective in addressing certain 5G cybersecurity risks identified in the EU coordinated risk assessment report.

The following eight strategic measures have been identified:

- SM01 Strengthening the role of national authorities;
- SM02 Performing audits on operators and requiring information;
- 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;
- SM04 Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support;
- SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies;
- SM06 Strengthening the resilience at national level;
- SM07 Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU;
- SM08 Maintaining and building diversity and EU capacities in future network technologies.

4.1.2 Technical measures include measures to strengthen the security of 5G networks and equipment by reinforcing the security of technologies, processes, people and physical factors. The effectiveness of the technical measures in terms of risk mitigation will vary depending on the scope of the measures and on the types of risks to be addressed. In particular, technical measures alone would not allow to address non-technical vulnerabilities (e.g. risk of interference by a third country or dependency risks).

The following 11 technical measures have been identified:

- TM01 Ensuring the application of baseline security requirements (secure network design and architecture);
- TM02 Ensuring and evaluating the implementation of security measures in existing 5G standards;
- TM03 Ensuring strict access controls;
- TM04 Increasing the security of virtualised network functions;
- TM05 Ensuring secure 5G network management, operation and monitoring;
- TM06 Reinforcing physical security;
- TM07 Reinforcing software integrity, update and patch management;
- TM08 Raising the security standards in suppliers' processes through robust procurement conditions;
- TM09 Using EU certification for 5G network components, customer equipment and/or suppliers' processes;
- TM10 Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services);

- TM11 Reinforcing resilience and continuity plans.

4.1.3. In addition, a set of targeted supporting actions have the potential to enable and assist the strategic and technical measures and thereby enhance their effectiveness:

- SA01 Reviewing or developing guidelines and best practices on network security;
- SA02 Reinforcing testing and auditing capabilities at national and EU level;
- SA03 Supporting and shaping 5G standardisation;
- SA04 Developing guidance on the implementation of security measures in existing 5G standards;
- SA05 Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme;
- SA06 Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers;
- SA07 Improving coordination in incident response and crisis management;
- SA08 Conducting audits of interdependencies between 5G networks and other critical services;
- SA09 Enhancing cooperation, coordination and information sharing mechanisms;
- SA10 Ensuring 5G deployment projects supported with public funding take into account cybersecurity risks

4.2. Risk mitigation plans

For each of the nine risk areas identified in the EU coordinated risk assessment report, the toolbox identifies and provides **risk mitigation plans**[30]. They consist of possible combinations of strategic and/or technical measures (together with the appropriate supporting actions) intended to mitigate a security risk.

The risk mitigation plans aim at providing guidance as to the **most relevant/high impact mitigation measures** based on an evaluation of the expected effectiveness of individual measures listed in section 4.1. to mitigate a particular risk. However, it should be noted that the expected effectiveness of most measures will depend highly on their scope and on the way they are implemented (for instance, strengthened regulatory powers have the potential to be highly effective, provided they have the appropriate scope and are used effectively).

In addition, risk mitigation plans reflect the importance of combining measures in an appropriate manner in order to ensure their full effectiveness and enforceability. Moreover, many of the measures, such as the application of enhanced security obligations on MNOs, require as a necessary pre-condition that regulatory authorities have the adequate powers to define and impose such obligations, as well as to monitor and audit their implementation.

These mitigation plans are presented in detail in annex 1 (table 2). An indicative high-level identification of other potential impact factors is also provided.

The estimated degree of **expected effectiveness** takes into account the original risk and the expected residual risk after applying the measure, and using the following scale:

- Very High: The measure is considered effective to a very high degree, meaning that it is expected to almost completely mitigate the related risks.

[30] In this context, a *risk mitigation plan* describes a possible approach that could be taken to mitigate a risk.

- High: The measure is considered highly effective, meaning that it is expected to significantly mitigate the related risks.
- Medium: The measure is considered somewhat effective, meaning that it is expected to mitigate the related risks to some extent.
- Low: The measure is considered hardly effective, as it is expected to mitigate the related risks only marginally.

In addition, for each measure, the table on mitigation plans (annex 1, table 2) indicatively identifies other parameters and characteristics, with a view of assisting Member States in selecting and implementing measures, namely:

- Potential **implementation factors** (can be positive and/or negative):
    - Resource costs
    - Sector-specific economic impacts (for operators or for suppliers)
    - Broader economic and/or societal impacts

- Indicative **timeframes** for taking the necessary steps to implement the measures, expressed using the following scale:
    - Short term: 0-2 years
    - Medium term: 2-5 years
    - Long term: >5 years

For ease of reference, a simplified visual representation of annex 1, table 2 is provided on the next page. Note that all indications regarding the expected effectiveness, potential impact factors and indicative timeframes given here are conditional and subject to the remarks and conditions as listed in the table 2 of annex 1. Please refer to the annex 1 for a more detailed information.

Table 3: simplified overview of measures in risk mitigation plans *(for more details, see annex 1, table 2)*

MEASURES	Indicative implementation timeframe			Potential implementation factors				SPECIFIC MEASURES	RISKS								
	Short-term	Medium-term	Long-term	Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal impact		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation
STRATEGIC MEASURES																	
a) Regulatory powers	✓			✓	✓	✓	✓	SM 01									
								SM 02									
b) Third party suppliers	✓			✓	✓	✓	✓	SM 03									
								SM 04									
c) Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM 05									
								SM 06									
d) Sustainability and diversity of 5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM 07									
								SM 08									
TECHNICAL MEASURES																	
a) Network security – baseline measures	✓			✓	✓			TM 01									
								TM 02									
b) Network security – 5G specific measures	✓			✓	✓			TM 03									
								TM 04									
								TM 05									
								TM 06									
								TM 07									
c) Requirements related to suppliers' processes and equipment		✓	✓	✓	✓	✓		TM 08									
								TM 09									
								TM 10									
d) Resilience and continuity	✓			✓	✓			TM 11									

Expected effectiveness:

Very low — Very high

5. Toolbox use and implementation

5.1. National and/or EU-level action

As outlined above, 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 risk posed by 5G. Measures may be implemented through national and/or EU-level actions, depending on the specific measure/actions. Some measures may be directly introduced or reinforced at national level, while others may require further action or joint action at EU level, in line with the respective competences.

The implementation of the **strategic measures may require** specific legislation at national level in order to fully achieve the impact of the measures. Some Member States have already implemented legislation related to these strategic measures and others are preparing similar legislation. In the future, coordination between Member States or at EU level may be beneficial in order to promote convergent approaches.

Measures to promote the sustainability and diversity of the 5G supply and value chain in order to avoid long-term dependencies require a concerted strategic approach, supported by the development of policies and legislation at EU level and/or the effective implementation of existing EU instruments to the 5G context (e.g. in the area of R&I or trade).

Many of the **technical measures** may be implemented in the context of the transposition of the European Electronic Communications Code. In terms of implementation and supervision of these measures, Member States will most likely need to cooperate in capacity building and would retain a level of discretion in supervision method and obligations. As some of these measures will be relevant to any 5G networks in a very similar manner, they may benefit from further enhanced EU cooperation and knowledge sharing, in particular through the review and development of guidelines and best practices and possibly from being further coordinated at EU level.

The supporting actions will not likely require legislative support. They will, however, require coordination in the same way.

5.2. Implementation of mitigation plans at national level

In selecting which measures are necessary to pursue, individual Member States will decide on the suitability of the measure. The Member State will also need to assess whether it has the resources to enforce the measure or if there is a need to cooperate with other Member States or at EU level.

The implementation of the measures by Member States will vary depending on a number of factors, such as the general characteristics of the national telecoms market (including the timeframe for deploying 5G networks, the presence of suppliers within networks and the degree of dependency on individual suppliers, the national resources and capabilities and the legal framework and security requirements already in place). Implementation plans may also specify transitional or gradual phases, in particular where a measure would result in a substantial shift from current practices.

Nonetheless, there are a number of overarching common parameters across Member States that make it possible to guide the selection and prioritisation of measures. These are provided through

the high-level grading of the effectiveness of measures, and through an indication on the various types of impact factors and the possible/desirable timeframe for the implementation of the measures, as outlined in annex 1 (table 2).

Table 4: How to use the toolbox

Step 1	Member State prioritises risks according to the national/EU Coordinated Risk Assessment.
Step 1a	Member State reviews the effectiveness of existing mitigations in addressing the risks in the Risk Assessment and identifies gaps.
Step 2	Member State identifies prioritised risks in table 2 (annex 1) to address the gaps identified in Step 1a.
Step 3	Member State studies the corresponding recommended measures and mitigation plans and selects the measure(s) that will have the most effect and considers potential implementation factors, alone or with aligned Member State(s).
Step 5	Member State implements all or parts of measure(s) accordingly, individually or with aligned Member State(s).

6. Conclusions and way forward

The EU toolbox sets out a range of measures and actions that – if appropriately combined and effectively implemented - form the basis for a coordinated approach in this area. Indeed, given the wide range of risk areas identified in the EU coordinated risk assessment and their different nature, no single type of measure will be sufficient and instead a range of measures used in an appropriate combination, will be necessary in order to address all key risk areas.

Based on the assessment of possible mitigation plans and the identification of the highest effectiveness measures, this toolbox recommends that:

1. All Member States should ensure that they have measures in place (including powers for national authorities) to respond appropriately and proportionately to the presently identified and future risks, and in particular ensure that they are able to restrict, prohibit, and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment, and operation of 5G network equipment on the basis of a range of security-related grounds.

They should in particular:

- 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 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;

2. The European Commission, jointly with Member states, should contribute to:

- Maintaining 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, in particular through the screening of potential foreign direct investments (FDIs) affecting 5G key assets and by avoiding distortions in the 5G supply market stemming from potential dumping or subsidies; and

    - 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.

3. To ensure that this coordinated approach stands the test of time, the mandate of the NIS Cooperation Group Work Stream should be extended, as well as the cooperation with other relevant bodies and entities, in order, in particular, to:

- Review periodically - with the support of the Commission and ENISA - the **national and EU risk assessments** on the security of 5G and post-5G networks, further elaborating and aligning the assessment methodology followed and adapting to the evolving 5G technology.

- Perform a detailed and regular **monitoring and evaluation of the implementation** of the toolbox based on a structured reporting by Member States;

- Coordinate and support the implementation of **supporting actions**, which require cooperation at EU level, in particular regarding the elaboration of guidance and exchange of best practices on the various measures.

- Support further possible coordination at EU-level where appropriate, in particular to bring further convergence as regards **technical and organisational security requirements for network operators**.

Annex 1 to the 5G EU toolbox of risk mitigating measures

- **Table 1: Strategic, technical measures & supporting actions**

STRATEGIC MEASURES					
Id	**Measure**	**Description**	**Related risks**	**Relevant actors**[31]	**Supporting actions**
SM01	**Strengthening the role of national authorities**	This should include regulatory powers for national authorities, to be able to: - impose strengthened obligations on operators, for example concerning the security of the signalling/management plane; - use *ex-ante* powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment, taking into account among other things: ▪ Security of critical and sensitive parts of 5G networks; ▪ Security of the equipment itself or the environment (deployment, interconnections, etc.); ▪ Risk of interference by a third country in the 5G supply chain; ▪ Risk of major dependency on a single supplier by individual MNOs or nationally ▪ Risks for national security.	R1 R2 R3 R4 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA01 SA04 SA06
SM02	**Performing audits on operators and requiring information**	In exercising their powers under Article 41(2) of the EECC[32], competent authorities should: - Audit, or require audits, of MNOs, if needed at an in-depth technical level, for example of critical components and/or sensitive parts of the 5G networks; - Require operators to provide detailed and up-to-date information about their plans for the sourcing of 5G equipment and for the involvement of third party suppliers;	R1 R2 R3 R4 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA02

[31] This column aims at identifying the main owners of the measures, i.e. actors responsible for developing, enforcing and/or implementing a measure.

[32] For specific new use cases in 5G (e.g. small closed 5G network serving critical functions such as, for example, a harbour or a hospital network) it is recommended to evaluate whether regulatory powers apply to these new type of MNOs and if not, to assess the need to regulate them.

		- Require operators to document and maintain a description on how the baseline technical network security measures are implemented[33].			
SM03	**Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risks-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[34] and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to: - Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other MS 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 profile.	R2 R5	▪ Relevant authorities ▪ Operators	SA06, SA10
SM04	**Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support**	Establish a legal/regulatory framework which places limit on the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers (MSPs), for both physical and virtual infrastructure, including: - Applying restrictions in particular in sensitive parts of the 5G networks, such as the security and network operations functions and where MSPs are considered to be high risk suppliers within the meaning of SM03; - For functions outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given to perform those functions.	R2 R5	▪ Relevant authorities ▪ Operators	SA06, SA10

[33] This may include security domains such as, for example, administrative information security, personnel security, security of hardware, software and telecommunications, security of information material and usage, physical security and other.

[34] The EU coordinated risk assessment report identifies several risk factors for the assessment of a supplier's risk profile, notably: the likelihood of the supplier being subject to interference from a non-EU country (this may be facilitated by, but not limited to, the presence of certain factors, which are also listed in the EU coordinated risk assessment report); the supplier's ability to assure supply; and the overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

		For equipment manufacturers' third line support during the design, deployment and/or operation of networks, impose strict access controls especially for critically sensitive components and/or sensitive parts of the network and in particular for suppliers considered to be high risk within the meaning of SM03.			
SM05	**Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies**	Ensure that each MNO has an appropriate multi-vendor strategy taking into account the technical constraints and interoperability requirements of the different parts of a 5G network: - To avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile); - To avoid dependency on suppliers considered to be high risk within the meaning of SM03.	R4	▪ Relevant authorities ▪ Operators	SA03, SA10
SM06	**Strengthening the resilience at national level**	Ensure that there is an adequate balance of suppliers at national level to ensure that there is resilience in case there is an incident with one operator and/or one supplier, taking into account the variations in geography and population in individual Member States.	R4	▪ Relevant authorities ▪ Operators	SA03, SA10
SM07	**Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU**	- Build on the EU's Foreign Direct Investment screening mechanism to improve the monitoring of FDI investments across the 5G value chain (e.g. through a mapping of key 5G assets, the use of monitoring tools and exploring specific guidelines), in order to better detect foreign investments in the 5G value chain that may pose a threat to the security or public order of more than one EU MS. Critical infrastructure, public security, access to and control of information and cybersecurity are well embedded under the scope of this (FDI) Regulation, allowing the evaluation of investments taking into account factors such as the risk profile of buyers/companies. - Should dependencies along the 5G value chain arise as a result of trade distorting market behaviour by producers falling under the scope and conditions of the relevant EU anti-dumping and/or anti-subsidy rules – and should these be notified via an ad hoc complaint or in exceptional circumstances via the European Commission's own initiative – then such behaviour could be investigated and acted upon through the EU's trade defence measures.	R4	▪ EC and Member States	SA10

SM08	**Maintaining and building diversity and EU capacities in future network technologies**	Develop policies which create optimal conditions for European technological firms and foster innovation in key technology areas to promote a diverse, sustainable and secure European 5G eco-system, including by: – Developing the proposed EU Institutionalised partnership in the field of NGI/6G ("Smart Networks and Services")[35] to ensure there is a sufficient degree of diversity of suppliers and sufficient knowledge and supply capacity in the EU across the telecoms value chain; - Developing EU capacities and therefore also avoid dependencies by supporting disruptive and ambitious research & innovation. This relates to the implementation of the various EU funding programmes, in particular Horizon Europe, the Digital Europe Programme and the Connecting Europe Facility (CEF) (e.g. through initiatives such as 5G Corridors for Connected and Automated Mobility); - Bringing together knowledge, expertise, financial resources and economic actors throughout the Union, so as to overcome potential important market or systemic failures along the value chain (IPCEI), and further specific industry initiatives.	R4	▪ EC and Member States ▪ All 5G stakeholders	SA10

TECHNICAL MEASURES

Id	Measures	Description	Related risks	Relevant actors	Supporting actions
TM01	**Ensuring the application of baseline security requirements (secure network design and architecture)**	Ensure that MNOs implement existing security best practices and recommendations non-specific to 5G networks on, for instance product development, configuration, day-to-day network management, incident management, security updates[36], for instance by imposing and reviewing risk assessment plans by MNOs. Ensure that MNOs keep up-to-date information on security policy, including operational information, as well as linked to change and	R1 R2 R3 R6 R7 R8 R9	▪ Relevant authorities ▪ Operators	SA01, SA05, SA09, SA10

[35] Proposed European Partnership for smart networks and services (Horizon Europe programme). Link to Inception Impact Assessment: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2019-4972300_en

[36] These measures should be based on international or European standards or technical guidelines, for example the Article 13a expert group guidelines of minimum security measures (https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf)

		incident management procedures for key network and information systems.			
TM02	**Ensuring and evaluating the implementation of security measures in existing 5G standards**	Ensure that MNOs and their suppliers implement the existing security measures in the relevant 5G technology standards (e.g. 3GPP)and use it as a minimum security baseline for MNOs, so as to ensure that also the optional parts of these standards, relevant for security, are adequately implemented	R1 R2 R3 R6 R7 R9	▪ Relevant authorities ▪ Operators ▪ Suppliers	SA03, SA04, SA05, SA10
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, virtualization configuration) are minimized; - 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 minimized and/or avoided whenever possible. When remote access is necessary, for example to address service outages, the MNO should apply appropriate authentication[37], authorization, logging and auditing so as to have a clear visibility on access to data and configuration changes or network alterations.	R1 R2 R3 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA05, SA10
TM04	**Increasing the security of virtualised network functions**	Ensure that MNOs follow security best practices for network function virtualisation. Note that there may be settings, for example when a network function is highly critical or when it is handling highly sensitive information, where virtualization is not appropriate and in such settings physical separation may be necessary.	R1 R3 R6 R7	▪ Relevant authorities ▪ Operators	SA01, SA05, SA10

[37] In terms of authentication general good practices apply and appropriate mechanisms should be used, for example for temporary access by third parties and/or remote access (e.g. no permanent credentials, temporary (one-time) passwords, usable only for designated tasks should be used). These measures could, for example, be enforced by using appropriate Privileged Access Management (PAM) platforms.

TM05	**Ensuring secure 5G network management, operation and monitoring**	Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU. The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT). Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.	R1 R2 R3 R5 R6 R7 R9	▪ Relevant authorities ▪ Operators	SA05, SA09, SA10
TM06	**Reinforcing physical security**	Ensure that MNOs reinforce physical protection of critical components and sensitive parts of the 5G networks, taking a risk-based approach for Multi-access Edge Computing (MEC) and base stations[38], for example considering where the components are deployed and used, like a MEC use in hospitals. In reinforcing physical access controls, it is important to ensure that access is granted only to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored, particularly where it concerns critical components and sensitive parts of the 5G networks.	R6 R7	▪ Relevant authorities ▪ Operators	SA05, SA10
TM07	**Reinforcing software integrity, update and patch management**	Ensure that MNOs deploy adequate tools and processes to ensure software integrity, which reliably identify and keep track of changes and the status of patches, when performing software updates and applying security patches in the 5G networks.	R1 R3 R5 R6 R7	▪ Relevant authorities ▪ Operators	SA02, SA10

[38] When doing the risk analysis, MNOs should consider the components and the service (like critical hospital MEC service).

TM08	**Raising the security standards in suppliers' processes through robust procurement conditions**	Ensure that MNOs demand specific security standards from equipment suppliers in the procurement process (e.g. on specific security improvements and demonstrating quality levels, security maintenance of the equipment throughout its lifetime and built-in of security in the product' development processes).	R3 R6 R7	▪ Relevant authorities ▪ Operators ▪ Suppliers	SA02, SA10
TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	The Commission should consider including into the Union Rolling Work Programme[39] relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework. It should also be examined at a later stage whether the certification or supplier's process could also be added to the Union Rolling Work Programme.	R3 R6 R7	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders	SA02, SA03 , SA09, SA10
TM10	**Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**	The Commission should consider including into the Union Rolling Work Programme EU-wide schemes under the EU certification framework for non-5G specific ICT products and services, such as for: - The security of cloud services and related technologies, which are an important part of 5G deployment[40]; - The security of connected (end-user) devices, including IoT.	R9	▪ Relevant authorities ▪ EC ▪ ENISA ▪ Stakeholders	SA02, SA03, SA09, SA10

[39] Under the EU cybersecurity certification framework, the Commission should publish the Union Rolling Work Programme for the development for the EU-wide certification schemes by July 2020.

[40] In accordance with Article 48(2) of the Cybersecurity Act, on 21 November 2019 the European Commission requested ENISA to prepare a candidate European cybersecurity certification scheme for cloud services.

TM11	**Reinforcing resilience and continuity plans**	Ensure that MNOs reinforce their resilience and continuity plans. MNOs should ensure they have adequate plans in place in case of disaster affecting the ongoing operation of their network, and ensure any critical dependencies are mapped and mitigated as required. MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.	R7 R8	▪ Relevant authorities ▪ Operators ▪ Suppliers ▪ Critical infrastructure operators	SA07, SA08, SA10

SUPPORTING ACTIONS

Id	Supporting action	Description	Relevant actors	Related measure(s)
SA01	**Reviewing or developing guidelines and best practices on network security**	Update the existing technical guidance on security measures for telecom providers based on Article 13a of the EU telecom framework directive and align it with Article 40 of the European Electronic Communications Code (EECC), taking also into account the need to develop best practices as regards new technologies and developments, such as Network Function Virtualisation (NFV).	▪ Relevant authorities ▪ ENISA ▪ Operators	SM01, TM01, TM04
SA02	**Reinforcing testing and auditing capabilities at national and EU level**	Reinforce competences, testing and auditing capabilities at national and/or EU level and, in particular: - Support the development of expertise of Information systems security audit service providers in telecom security audits through capacity building and EU investment in training; - The Commission should consider including into the Union Rolling Work Programme the development of an EU certification scheme for cybersecurity audit service providers in particular to support the development of capability for in-depth technical audits and security evaluations in co-operation between MS and facilitate sharing information on benchmarks of certified audit service providers. Union level framework for technical audits and security evaluation will give better position to require security from suppliers.	▪ Relevant authorities ▪ EC ▪ ENISA	SM02, TM07, TM08, TM09, TM10

SA03	**Supporting and shaping 5G standardisation**	Increase engagement in relevant standardisation bodies, in particular through reinforced coordination at EU level in order to increase ability to shape standardisation according to identified needs, by setting up a forum or group of national regulatory authorities and other relevant competent authorities of Member states, reporting to the NIS Cooperation Group and the EECG[41], in particular tasked to: - Contribute to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification, in line with existing legislation, such as but not limited to the Cybersecurity Act; - Promote standardisation of interfaces to facilitate diversity of suppliers; - ensure liaison between the NIS Cooperation Group and relevant European and/or international standardisation bodies; - Ensure full participation by EU industry and improve the dialogue between the industry and the MS.	▪ Relevant authorities ▪ EC ▪ Operators ▪ Suppliers ▪ ENISA	SM05, SM06, TM02, TM09, TM10
SA04	**Developing guidance on implementation of security measures in existing 5G standards**	Develop specific EU guidance on the implementation of security measures under the existing 5G standards (e.g. 3GPP), and in particular: - Provide recommendations on the optional elements of standardisation and on aspects that are not covered by a specific standard;[42] - Identify existing gaps in telecommunications standardisation of architectures/functionalities for mitigating identified risks.	▪ Relevant authorities ▪ ENISA	SM01, TM02
SA05	**Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme**	Consider developing an EU-wide certification scheme under the EU certification framework for information security management systems (ISMS) for telecommunication providers.	▪ Relevant authorities ▪ ENISA ▪ Stakeholders	TM01 to 06
SA06	**Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing**	To facilitate a coordinated approach, exchange good practices on the implementation of strategic measures, in particular on the risk factors to be taken into account (see paragraph 2.37 of the EU coordinated risk assessment report) when assessing the risk profile of suppliers/vendors. In addition to the factors listed in the EU coordinated risk assessment report, these factors could include national-specific information such as market penetration of suppliers, threat intelligence from national security services, etc.	▪ Relevant authorities	SM01, SM03, SM04

[41] The European Cybersecurity Certification Group (EECG) set up under the Cybersecurity Act is composed representatives of national cybersecurity certification authorities or representatives of other relevant national authorities.

[42] This may include, for example, aspects such as deployment/hosting options, recommended commercial off-the-shelf (COTS) software and hardware architectures and configurations, monitoring procedures or any other aspects.

	the risk profile of suppliers			
SA07	**Improving coordination in incident response and crisis management**	Through the ongoing work within the dedicated NIS Work stream, ensure there are good cooperation and coordination mechanisms between the relevant national authorities and at EU level when dealing with large-scale cross-border cybersecurity incidents and crises, on the basis of the Blueprint[43]. Moreover, to prepare for large-scale incidents involving 5G networks, Member States could consider including 5G scenarios in national as well as EU-wide cyber exercises, where appropriate.	▪ Relevant authorities ▪ ENISA	TM11
SA08	**Conducting audits of interdependencies between 5G networks and other critical services**	Analyse critical dependencies between the 5G networks and other critical sectors, such as electricity supply, as well as sectoral dependencies for 5G, such as drinking water and transportation. This should also consider circular dependencies (e.g. 5G network dependent on power supply and, at the same time, power being dependent on 5G network).	▪ Relevant authorities	TM11
SA09	**Enhancing cooperation, coordination and information sharing mechanisms**	Consider the use of existing cooperation, coordination and information sharing mechanisms, including actions and support by ENISA, notably through regular threat assessments.	▪ Relevant authorities ▪ ENISA	TM01, TM05, TM09, TM10

[43]Commission Recommendation on a coordinated response to large-scale cybersecurity incidents & crisis (EU 2017/1584).

SA10	**Ensuring 5G projects supported with public funding take into account cybersecurity risks**	Develop detailed guidelines for 5G-related security provisions in public procurement and EU funding programmes (Horizon, Connecting Europe Facility, Digital Europe Programme). These guidelines could be prepared within the comitology procedure by committee members nominated by Member States in the course of preparing the annual work programmes under the different funding programmes. Public funding programmes such as the Connecting Europe Facility (CEF) Digital are expected to play a key role in shaping the deployment of 5G networks in Europe, e.g. 5G Corridors for Connected and Automated Mobility as well as 5G Connectivity for Socio-Economic Drivers. Therefore the above-mentioned guidelines should be used in the implementation of these programmes. In particular, when consortia for such projects are set up with participation or administrative support by public authorities, where cyber-security risks (in particular risks identified in the EU coordinated risk assessment report and the relevant mitigation measures described in this toolbox) are identified, those should be taken into consideration when selecting suppliers or other project participants. At national level, in the area of public procurement, the EU Directives and policies encourage Member States to not award contracts solely on the basis of the lowest price, but also take into account quality in areas such as security, labour and environmental standards. Moreover, the Commission Recommendation of 26 March, 2019 refers specifically to the possible development and implementation of European cybersecurity certification schemes in public procurement related to 5G networks.	▪ Relevant authorities ▪ EC	SM03 to 08 TM01 to 11

- # Table 2: Risk mitigation plans

Table 2 below presents risk mitigation plans for each of the nice risk areas identified in the EU coordinated risk assessment report.

The estimated degree of **expected effectiveness** takes into account the original risk and the expected residual risk after applying the measure, and using the following scale:

- Very High: The measure is considered effective to a very high degree, meaning that it is expected to almost completely mitigate the related risks.
- High: The measure is considered highly effective, meaning that it is expected to significantly mitigate the related risks.
- Medium: The measure is considered somewhat effective, meaning that it is expected to mitigate the related risks to some extent.
- Low: The measure is considered hardly effective, as it is expected to mitigate the related risks only marginally.

In addition, for each measure, the table on mitigation plans (annex 1, table 2) indicatively identifies other parameters and characteristics, with a view of assisting Member States in selecting and implementing measures, namely:

- Potential **implementation factors** (both positive and negative), namely:
    - Resource costs
    - Sector-specific economic impacts (for operators or for suppliers)
    - Broader economic and/or societal impacts

- Indicative **timeframes** for taking the necessary steps to implement the measures, expressed using the following scale:
    - Short term: 0-2 years
    - Medium term: 2-5 years
    - Long term: >5 years

Risk 1: **Misconfiguration of Networks** Risk mitigation plan: Increase network security and resilience			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on implementation of measures, but can be **VERY HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers) ▪ (potentially) Broader economic and/or societal impacts	**SHORT** term
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM** to **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM03: Ensuring strict access controls TM04: Increasing the security of virtualised network functions TM05: Ensuring secure 5G network management, operation and monitoring TM07: Reinforcing software integrity, update and patch management	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.
Risk 2: **Lack of Access Controls** Risk mitigation plan: Increase network security, in particular **strengthen rules on access to network by suppliers and on use of Managed Service Providers and third line support**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on implementation of measures, but can be **VERY HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators) ▪ (potentially) Broader economic and/or societal impacts	**SHORT** term
Third party suppliers: SM03: Assessing the risk profile of suppliers and for suppliers considered to be high risk, applying restrictions, including necessary exclusions, for key assets	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)	**SHORT** term. Depends on 5G deployment calendar.

SM04: Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support		▪ (potentially) Broader economic and/or societal impacts	
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM03: Ensuring strict access controls TM05: Ensuring secure 5G network management, operation and monitoring	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators)	**SHORT** term. Depends on 5G deployment calendar.
Risk 3: **Low equipment quality** Risk mitigation plan: Apply **pressure or incentives on suppliers to increase product quality and increase network security and resilience**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be HIGH or **VERY HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators) ▪ (potentially) Broader economic and/or societal impacts	**SHORT** term
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM03: Ensuring strict access controls TM04: Increasing the security of virtualised network functions TM05: Enforcing secure 5G network management, operation and monitoring TM07: Reinforcing software integrity, update and patch management	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)	**SHORT** term. Depends on 5G deployment calendar.
Requirements related to suppliers' processes and equipment TM08: Raising the security standards in suppliers' processes through robust procurement conditions TM09: Using EU-wide certification for 5G network components and/or suppliers' processes	**MEDIUM** (possibly HIGH at a long term)	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)	**MEDIUM and LONG** term

Risk 4: **Dependency on a single supplier** Risk mitigation plan: **Ensure diversity of supply within each operator and geographical balance at national level and promote long-term sustainability of 5G supply chain**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be **HIGH or VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators) (potentially) Broader economic and/or societal impacts	**SHORT** term
Diversification of suppliers: SM05: Ensuring the diversity of suppliers for individual MNOs, through appropriate multi-vendor strategies SM06: Strengthening the resilience at national level	Depends on scope of measure but can be **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)[44] ▪ (potentially) Broader economic and/or societal impacts	**SHORT to MEDIUM** term. Depends on 5G deployment calendar.
Sustainability and diversity of 5G supply and value chain: SM07: Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU SM08: Maintaining and building diversity and EU capacities in future network technologies	Depends on scope of measures but can be **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers) ▪ (potentially) Broader economic impacts	**SHORT, MEDIUM** and **LONG** term
Risk 5: **State interference through 5G supply chain** Risk mitigation plan: Restrict the use of **high risk suppliers and strengthen access controls, network monitoring and patch management processes**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be **HIGH** or **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators)	**SHORT** term

[44] For the measure SM05, sector-specific economic impact will also depend on on existing level of diversity

		▪ (potentially) Broader economic and/or societal impacts	
Third party suppliers: SM03: Assessing the risk profile of suppliers and for suppliers considered to be high risk, applying restrictions, including necessary exclusions, for key assets SM04: Controlling the use of Managed Service Providers (MSPs) and vendor third line support	Depends on scope of measures and exposure to high risk suppliers but can be **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers) ▪ (potentially) Broader economic and/or political impacts	**SHORT** term. Depends on 5G deployment calendar
Network security – 5G specific measures TM03: Ensuring strict access controls TM05: Ensuring secure 5G network management, operation and monitoring TM07: Reinforcing software integrity, update and patch management	If taken as standalone measure can be **MEDIUM**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.
Risk 6: **Exploitation of 5G networks by organised crime** Risk mitigation plan: **Increase network security and raise quality of supplier's processes and equipment**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be High or **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators) ▪ (potentially) Broader economic and/or societal impacts	**SHORT** term
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM TO HIGH**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM03: Ensuring strict access controls TM04: Increasing the security of virtualised network functions TM05: Ensuring secure 5G network management, operation and monitoring TM06: Reinforcing physical security TM07: Reinforcing software integrity, update and patch management	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.

Requirements related to suppliers' processes and equipment TM08: Raising the security standards in suppliers' processes through robust procurement conditions TM09: Using EU-wide certification for 5G network components and/or suppliers' processes	**MEDIUM** (possibly HIGH in the long term)	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)	**MEDIUM and LONG** term
Risk 7: **Significant disruption of critical infrastructure or services** Risk mitigation plan: **Increase network security, ensure resilience and continuity and raise quality of supplier's processes and equipment**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be HIGH or **VERY HIGH**	▪ Resource costs ▪ Sector-specific economic impacts (operators) ▪ (potentially) Broader economic and/or societal impacts	**SHORT** term
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM TO HIGH**	▪ Resource costs Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM03: Ensuring strict access controls TM04: Increasing the security of virtualised network functions TM05: Ensuring secure 5G network management, operation and monitoring TM06: Reinforcing physical security TM07: Reinforcing software integrity, update and patch management	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.
Requirements related to suppliers' processes and equipment: TM08: Raising the security standards in suppliers' processes through robust procurement conditions TM09: Using EU-wide certification for 5G network components and/or suppliers' processes	**MEDIUM** (possibly HIGH in the long term)	▪ Resource costs ▪ Sector-specific economic impacts (operators and suppliers)	**MEDIUM and LONG** term
Resilience and continuity: TM11: Reinforcing resilience and continuity plans	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.

Risk 8: **Massive failure of networks due to interruption of electricity supply** Risk mitigation plan: **Ensure resilience and continuity and increase network security**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture)	Depends on implementation, but can be **HIGH**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Resilience and continuity: TM11: Reinforcing resilience and continuity plans	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.
R9: **IoT exploitation** Risk mitigation plan: **Increase network security and improve security of end user IoT devices**			
Most relevant/high-impact measures	**Expected effectiveness**	**Potential implementation factors**	**Indicative timeframe**
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be **MEDIUM**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term
Network security – 5G specific measures TM05: Ensuring secure 5G network management, operation and monitoring	Depends on scope of measures, but can be **HIGH.**	▪ Resource costs ▪ Sector-specific economic impacts	**SHORT** term. Depends on 5G deployment calendar.
Requirements related to suppliers' processes and equipment TM10: Using certification for other non 5G-specific ICT products and services (connected devices, cloud services)	**HIGH**	▪ Resource costs ▪ Sector-specific economic impacts	**MEDIUM and LONG** term

Annex 2- Summary of the findings of the EU coordinated risk assessment[45]

The EU coordinated risk assessment follows the approach set out in the ISO/IEC: 27005 risk assessment methodology. It reflects the assessment of a set of parameters:

- The main types of threats posed to 5G networks;
- The main threat actors;
- The main assets and their degree of sensitivity;
- The main vulnerabilities; and
- The main risks and related scenarios.

Threats, assets and vulnerabilities

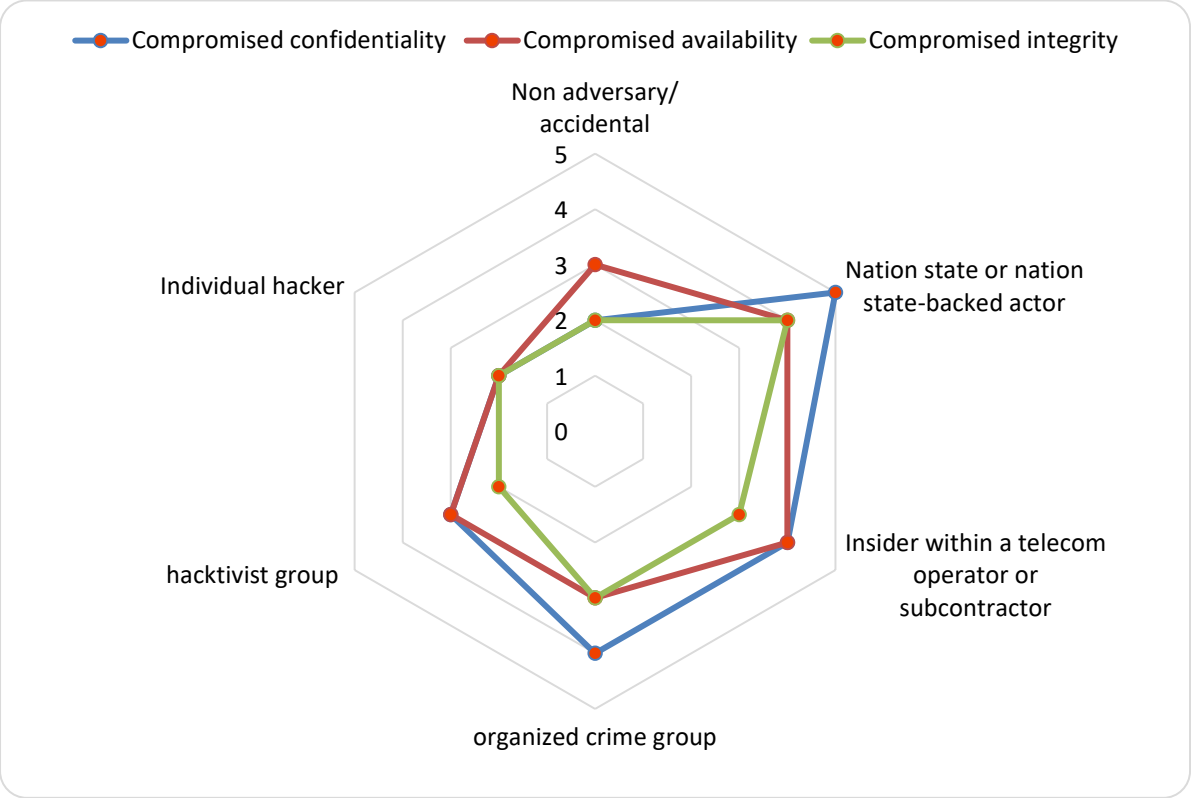


Figure 1 - Consolidated view on threat category by threat actor

-Threats

Threats posed by states or state-backed actors, are perceived to be of highest relevance. They represent indeed the most serious as well as the most likely threat actors, as they can have the motivation, intent and most importantly the capability to conduct persistent and sophisticated attacks on the security of 5G networks.

[45] Full report: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

The combination of motivation, intent and a high-level capability enables states to perpetrate attacks that can be very complex and have a major impact on essential services for the general public, deteriorating the trust in mobile technologies and operators. For example, states or state-backed actors can cause large-scale outage or significant disturbance of telecommunications services by exploiting undocumented functions or attacking interdependent critical infrastructures (e.g. power supply).

In relation to state and state-backed actors, a particular threat stems from cyber offensive initiatives of non-EU countries. Several Member States have identified that certain non-EU countries represent a particular cyber threat to their national interests, based on previous *modus operandi* of attacks by certain entities or on the existence of an offensive cyber programme of a given third state against them.

It is also noted that insiders or subcontractors can in certain circumstances also be considered potential threat actors, especially if leveraged by states as they could be used as a channel for a state to gain access to critical target assets.

Further categories of actors could also be considered to have an important motivation to target 5G networks in order to serve their interest, i.e. organised crime groups, corporate entities seeking to gain competitive advantage in the technological field through Intellectual Property (IP) theft or cyber terrorists.

-Network assets

CATEGORIES OF ELEMENTS AND FUNCTIONS		EXAMPLES OF KEY ELEMENTS
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions
		User Equipment data transport functions
		Access policy management
		Registration and authorization of network services
		Storage of end-user and network data
		Link with third-party mobile networks
		Exposure of core network functions to external applications
		Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems
		Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations

Transport and transmission functions	**MODERATE/HIGH**	Low-level network equipment (routers, switches, etc)
		Filtering equipment (firewalls, IPS...)
Internetwork exchanges	**MODERATE/HIGH**	IP networks external to MNO premises Network services provided by third parties

Core network functions of the 5G network are generally considered as critical. Indeed, affecting the core network may potentially compromise the confidentiality, availability and integrity of the entire network services (whereas compromises of other components may have a more limited impact, e.g. affecting only a specific function or area). Furthermore, the most sensitive data is transmitted through the core network components.

Management systems and supporting services (MANO and other management systems and supporting services) are considered as important even though these systems do not carry traffic since they control important network elements and can therefore be used to conduct malicious acts, such as sabotage and espionage of serious consequences. Moreover, the loss of availability or integrity of these systems and services can disrupt significantly the functioning of 5G networks.

Among the core functions and management systems/supporting services, a number of elements and functions have been considered to be of particularly high importance, notably: the NFV Management and Network Orchestration (MANO), core access and control functions, security functions, lawful interception functions, cryptographic infrastructures necessary to configure and operate 5G networks and specific management functions.

Access network functions were also rated with relatively high sensitivity. However, the assessment of the degree of sensitivity of specific elements within the access functions varies according to a number of factors. Furthermore, in the coming development phases of 5G, traditionally less sensitive parts of the network are gaining importance and becoming more sensitive, such as for instance certain elements in the radio access part of the network, depending on the extent to which they handle user data or perform smart or sensitive functions. Moreover, when edge computing is introduced, certain core network functions are expected to be moved physically farther out in the network, closer to the access sites.

Transport and transmission functions were rated as moderately to highly sensitive. However, similarly to the access functions, the assessment of the degree of sensitivity of specific elements within the transport and transmission functions varies according to a number of factors.

Internetwork exchanges functions were rated as moderately to highly sensitive, depending on their role in the interconnection between MNOs.

-Other assets

When considering key assets, a number of entities and categories of users can be considered as requiring particular attention, namely:

- Operators of essential services under NIS Directive and critical infrastructure operators;
- Government entities, law enforcement, Public Protection and Disaster Relief (PPDR), military;
- Key sectors/entities not covered by cybersecurity regulations;
- Strategic private companies; and
- Areas or entities for which there is no back-up solution in place in case of 5G network failure.

In addition, a number of Member States have identified geographic areas that are particularly sensitive, based on an analysis of the demographic, economic, societal and national security factors. Indeed, certain areas could suffer greater disruption due to the concentrations of economic and societal reliance on network and information systems (e.g. as in the case of smart cities) or because sensitive entities or categories of users are located in them.

-Vulnerabilities

The report assessed three main types of vulnerabilities:

1. Vulnerabilities related to hardware, software, processes and policies

As any digital infrastructure, 5G networks can be associated with a range of generic technical vulnerabilities, which may affect software, hardware or arise from potential deficiencies in the security processes of any of the various stakeholders[46]. Furthermore, in the early stage of deployment, vulnerabilities in the existing 3G and 4G infrastructure shall also be duly considered.

While many of these vulnerabilities are not specific to 5G networks, their number and significance is likely to increase with 5G, due to the increased level of complexity of the technology and of the future greater reliance of economies and societies on this infrastructure.

When it comes to process or configuration-related vulnerabilities are considered to be of special significance in the future 5G environment:

For all stakeholders, in particular mobile network operators and their suppliers:

- Lack of specialised and trained personnel to secure, monitor and maintain 5G networks;
- Lack of adequate internal security controls, monitoring practices, security management systems and insufficiencies in risk management practices;
- Lack or inadequate security or operational maintenance procedures, such as software update/patch management; and
- Lack of compliance with 3GPP standards or incorrect implementation of standards.

[46] Reviews of the practices of one of the major network equipment suppliers as regards 4G equipment and services have been for instance carried out by the UK Huawei Cybersecurity Evaluation Centre (HSCEC).

For mobile network operators:

- Poor network design and architecture;
- Poor physical security for network and IT infrastructure;
- Poor policies for local and remote access to network components;
- Lack of or insufficient security requirements in the procurement process; and
- Poor change management process.

2. Supplier-specific vulnerabilities

The increased role of software and services provided by third party suppliers in 5G networks leads to a greater exposure to a number of vulnerabilities that may derive from the risk profile of individual suppliers. The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

- The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks[47]. Such interference may be facilitated by, but not limited to, the presence of the following factors:
    - A strong link between the supplier and a government of a given third country;
    - The third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country[48];
    - The characteristics of the supplier's corporate ownership; and
    - The ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.
- The supplier's ability to assure supply.
- The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

The assessment of a supplier's risk profile may also take into account notices issued by EU authorities and/or Member States national authorities.

3. Vulnerabilities stemming from dependency to individual suppliers

Within individual networks, a large degree of reliance on a single supplier (monoculture) creates a dependency on specific solutions and makes it more difficult to procure solutions from other suppliers, especially where solutions are not fully interoperable.

As a result, EU-based operators who become overly dependent on a single equipment supplier are exposed to a number of risks caused by that supplier coming under sustained

[47] While a threat actor's direct access to or influence on the telecom supply chain may significantly facilitate its exploitation for malicious actions and make the impact of such actions significantly more severe, it should also be noted that actors with a high level of intent and capabilities, such as State actor, would seek to exploit vulnerabilities at any stage of the product lifecycle provided by any supplier.

[48] In this context, several Member States attribute a higher risk profile to suppliers that are under the jurisdiction of third countries conducting an offensive cyber policy.

commercial pressure, whether due to commercial failure, being subject to a merger or acquisition, or being placed under sanctions.

At national and EU level, a lack of diversity of suppliers increases the overall vulnerability of the 5G infrastructure, in particular if a large number of operators source their sensitive assets from a supplier presenting a high degree of risk, as described above. Dependency of one or several networks also significantly affects national and EU-wide resilience and creates single points of failure.

Moreover, the presence of a limited number of suppliers on the market can decrease their incentives to develop more secure products. It can also have a negative impact on the leverage available to national authorities and operators to demand higher security guarantees, in particular for smaller Member States or operators.

Main risks and risk scenarios

The EU coordinated risk assessment identified several main risk categories illustrated by concrete risk scenarios, describing possible attacks paths that a threat actor can use to reach its target:

I - Risk scenarios related to insufficient security measures	**R1-**Misconfiguration of networks: Exploiting poorly configured systems and architecture, a State actor penetrates into the 5G network via its external interfaces, leading to the compromise of the network core functions, or exploits edge-computing nodes in order to compromise information confidentiality and disrupt distributed services. **R2-**Lack of access controls: A subcontractor with administrator's privileges on the network performs adverse action, leading to confidentiality/integrity and/or availability breach. The subcontractor's action may be due to a legal requirement imposed by a third country or rogue behaviour of the contractor's staff.
II – Risk scenarios related to 5G supply chain	**R3-**Low product quality: Espionage by state or state-backed actors using malware to abuse poor quality network components or unintentional vulnerabilities affecting sensitive elements in the core network, such as Network Virtualisation Functions. **R4-**Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis: A mobile network operator sources a large amount of its sensitive network components or services from a single supplier. The availability of equipment and/or updates from this supplier is subsequently drastically reduced, due to a failure by the supplier to supply (e.g. due to trade sanctions by a third State or to other commercial circumstances). In consequence, the quality of a supplier's equipment decreases due to priority given to guaranteeing supply over improvements in product security.
III - Risk scenarios related to modus	**R5-** State interference through 5G supply chain: A hostile state actor exercises pressure over a supplier under its jurisdiction to

operandi of main threat actors	provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities. **R6-** Exploitation of 5G networks by organised crime or Organised crime group targeting end-users: By taking control of a critical part of the 5G network architecture, an organized crime group disrupts various services to ransom businesses relying on those services, or the mobile network operator itself. Alternatively, using a similar attack path, an organised crime group may also target end-users, e.g. by injecting false messages to the users of the network as part of a large-scale "phishing" attack or online scam, or by using the compromised network to gain access to confidential data about users (e.g. second-factor authentication codes) for further profit.
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	**R7-** Significant disruption of critical infrastructures or services: Malicious hackers are able to compromise emergency services by gaining control of their dedicated network slice, thus compromising the availability of the service and the integrity of the information/data used for/within that service. **R8**-Massive failure of networks due to interruption of electricity supply or other support systems: Massive outage of power supply due to natural disasters or to attacks to the energy grid by a state, a state-backed actor or an organised crime group.
V - Risk scenarios related to end user devices	**R9-**IoT (Internet of Things) exploitation: A hacktivist group or state-backed actor takes control of low security devices like IoT (sensors, home appliances, etc.), in order to attack the network by overwhelming its signalling plane.

Conclusions of the EU coordinated risk assessment

The EU coordinated risk assessment highlights a number of important security challenges, which are likely to appear or become more prominent in 5G networks, compared with the situation in existing networks. These security challenges are mainly linked to:

- Key innovations in the 5G technology (which will also bring a number of specific security improvements), in particular the important part of software and the wide range of services and applications enabled by 5G;
- The role of suppliers in building and operating 5G networks and the degree of dependency on individual suppliers.

Specifically, the roll-out of 5G networks is expected to have the following effects:

- An increased exposure to attacks and more potential entry points for attackers: With 5G networks increasingly based on software, risks related to major security flaws, such as those deriving from poor software development processes within suppliers are gaining in importance. They could also make it easier for threat actors to maliciously insert backdoors into products and make them harder to detect.

- Due to new characteristics of the 5G network architecture and new functionalities, certain pieces of network equipment or functions are becoming more sensitive, such as base stations or key technical management functions of the networks.

- An increased exposure to risks related to the reliance of mobile network operators on suppliers. This will also lead to a higher number of attacks paths that might be exploited by threat actors and increase the potential severity of the impact of such attacks. Among the various potential actors, non-EU states or state-backed are considered as the most serious ones and the most likely to target 5G networks.

- In this context of increased exposure to attacks facilitated by suppliers, the risk profile of individual suppliers will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country.

- Increased risks from major dependencies on suppliers: a major dependency on a single supplier increases the exposure to a potential supply interruption, resulting for instance from a commercial failure, and its consequences. It also aggravates the potential impact of weaknesses or vulnerabilities, and of their possible exploitation by threat actors, in particular where the dependency concerns a supplier presenting a high degree of risk.

- Threats to availability and integrity of networks will become major security concerns: in addition to confidentiality and privacy threats, with 5G networks expected to become the backbone of many critical IT applications, the integrity and availability of those networks will become major national security concerns and a major security challenge from an EU perspective.

The report further concludes that these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem and essential for Member states to take the necessary mitigating measures.