EUROPEAN
COMMISSION

Brussels, 16.12.2020
SWD(2020) 357 final

COMMISSION STAFF WORKING DOCUMENT

Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks

COMMISSION STAFF WORKING DOCUMENT

Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks

Contents

Introduction

The fifth generation (5G) of telecommunication networks is set to play an essential role in the development of the European society and economy. It is expected to offer vast economic opportunities and to be an important basis for the digital and green transformation in areas such as transport, energy, manufacturing, health, agriculture and media. 5G technology and standards are evolving in several phases, as deployment advances. Operators in more than half of the European Union (EU) Member States have already launched commercial 5G networks in major cities, whereas a more comprehensive deployment covering all urban areas and major transport paths across Europe is expected by 2025.

At the same time, the proliferation of connected devices, our high reliance on digital technologies especially during the COVID-19 pandemic, and the rollout of very high capacity communications infrastructure such as 5G networks, give rise to new vulnerabilities and risks. The interconnected and transnational nature of these infrastructures mean that any significant vulnerabilities and/or cybersecurity incidents concerning 5G networks happening in one Member State could have significant impacts beyond national borders and would

affect the Union as a whole. As a result, ensuring the cybersecurity and resilience of 5G networks is an issue of strategic importance for the Union.

Member States expressed their support for a coordinated approach to the cybersecurity of 5G networks in the European Council conclusions of 22 March 2019. Following the European Council's call for collective action, the European Commission adopted its Recommendation on the cybersecurity of 5G networks[1] ('The Recommendation') on 26 March 2019. This marked the start of a process aimed at ensuring the solid and long-term cybersecurity of 5G networks in the EU, following a coordinated approach. Over the past one and a half year, Member States worked together to deliver on the various steps outlined in the Recommendation, with the help of the Commission and the EU Agency for Cybersecurity (ENISA) in the framework of the Security of Network and Information Systems (NIS) Cooperation Group, which brings together national authorities responsible for cybersecurity.

The Recommendation fits into a broader European legal framework for the protection of electronic communications networks and their ecosystem, notably the European Electronic Communications Code[2] which demands that all electronic communications service providers take appropriate security measures. In addition, the Cybersecurity Act[3] creates a framework for the development of cybersecurity certification schemes for products, processes and services, and the Directive on security of network and information systems (NIS Directive)[4] lays out security requirements for operators of essential services (other than telecoms). Rules have also been defined at Union level ensuring the security of processing of personal data, including in electronic communications, notably the General Data Protection Regulation[5] and the e-Privacy Directive[6]. This framework is complemented by EU rules on public procurement[7] and foreign direct investment screening[8].

Content and objective of the report

The objective of this report is to assess the impacts of the Recommendation and determine appropriate ways forward, as set out in Article 19 of the Recommendation. This article

[1] Recommendation (EU) 2019/534 on the cybersecurity of 5G networks, OJ L 88, 29.3.2019, p. 42–47.
[2] Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, p. 36–214.
[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.
[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.
[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37.
[7] 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 third country bidders and goods in the EU procurement market.
[8] Regulation (EU) 2019/452 of 19 March, 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ L 79I , 21.3.2019, p. 1–14.

provides that this assessment should take into account the outcome of the coordinated Union risk assessment and the Union Toolbox.

To this end, this report looks back at the various steps achieved and how Member States perceived the process initiated by the Recommendation. The report also provides an update on the implementation of the Toolbox measures. This information is notably based on data collected during bilateral 'country meetings' with Member State authorities, conducted by the Commission with the support of ENISA in autumn 2020 and on various other meetings held with Member States authorities at EU level.

Moreover, it describes the state of play of the Supporting actions (SA) undertaken by the Commission and ENISA, in the fields of standardisation and certification, EU funding for secure 5G roll-outs, actions to promote EU capacities in the area of network technology, and fostering a diverse and sustainable 5G ecosystem in the EU.

The conclusions of this review led to the identification of key objectives and specific actions for the future coordinated work at Union level on 5G cybersecurity, which are set out in the Joint Communication 'The EU's Cybersecurity Strategy for the Digital Decade'[9] and its dedicated Annex, published on the same day as this report.

1. Overall process

1.1. Main steps taken to implement the Recommendation

The Recommendation set out a number of concrete steps, which were completed following a defined schedule (between April 2019 and January 2020).

Specifically, the Recommendation has the general objective *"to support the development of a Union approach to ensuring the cybersecurity of 5G networks"* and identifies "*actions which should be taken to enable:*

> *(a) Member States to assess the cybersecurity risks affecting 5G networks at national level and take necessary security measures.*
> *(b) Member States and relevant Union institutions, agencies and other bodies to develop jointly a coordinated Union risk assessment that builds on the national risk assessment.*
> *(c) The Cooperation Group set up under Directive (EU) 2016/1148 (Cooperation Group) to identify a possible common set of measures to be taken to mitigate cybersecurity risks related to infrastructures underpinning the digital ecosystem, in particular 5G networks".*

First, in spring 2019, each Member State performed a national risk assessment of 5G network infrastructures. The results were shared with other Member States, the Commission and ENISA, following commonly defined guidelines and a common template in July 2019. The

[9] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18.

national risk assessments formed the basis for the EU Coordinated risk assessment[10] published by the NIS Cooperation Group on 9 October 2019. This Coordinated risk assessment identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities[11] and the main associated risks, illustrated by concrete risk scenarios. To complement the Coordinated risk assessment, ENISA published a dedicated Threat Landscape mapping[12], which contained a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting them specifically. This report[13] has been updated by ENISA on 14 December 2020.

The assessment of the risks led to the development of the EU 5G Toolbox of mitigating measures and plans[14] ('The Toolbox'), published on 29 January 2020. The Toolbox contains a set of Strategic and Technical measures, aimed at mitigating 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.

In its Communication[15] accompanying the Toolbox, the Commission endorsed the measures recommended in the Toolbox conclusions and underlined the importance of their effective and swift implementation. It called on Member States to take concrete first steps to implement the Toolbox measures by 30 April 2020. The implementation was assessed in the Progress report[16] published by the NIS Cooperation Group in July 2020.

In October 2020, the European Council called on the EU and the Member States "*to make full use of the 5G cybersecurity Toolbox adopted on 29 January 2020, and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments, based on common objective criteria"*[17].

Other relevant entities have been involved at national and Union level in the process launched by the 2019 Recommendation. In particular, the Body of European Regulators for Electronic Communications (BEREC) cooperated with the NIS Cooperation Group, notably by providing input for the preparation of the Toolbox and its implementation. In November 2019, BEREC also organised a workshop with industry stakeholders' representatives, in order to inform them about the preparation of the Toolbox and gather their views. The Commission and ENISA regularly liaised with and informed other groups of Member States

[10] EU-wide coordinated risk assessment of 5G networks security, 9 October 2020, https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[11] 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.

[12] ENISA Threat landscape for 5G networks, 21 November 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

[13] ENISA Threat landscape for 5G networks - Updated threat assessment for the fifth generation of mobile telecommunications networks, 14 December 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/

[14] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[15] Secure 5G deployment in the EU-Implementing the EU Toolbox, COM(2020) 50 final.

[16] Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, 24 July 2020, https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

[17] EUCO 13/20, Special meeting of the European Council (1 and 2 October 2020) – Conclusions.

authorities, including the Article 13a Expert Group, the Communications Committee and the relevant Council Working Parties.

1.2. Member States' views on the process

Member States were highly appreciative of the overall process and found that it enabled an unprecedented method of cooperation leading to the definition of an ambitious and coordinated EU framework for 5G cybersecurity, while preserving flexibility in view of the national security aspects. They qualified Europe's coordinated action on 5G cybersecurity as timely, effective and proportionate. The collaborative approach between national authorities, the Commission, ENISA and other relevant stakeholders was considered suitable to address this complex issue that cuts across EU and Member State competences. It allowed the timely definition of common objectives and methodologies, while allowing Member States to adapt measures to their national circumstances. The urgency and importance of this matter was fully recognised and led to the mobilisation of all relevant actors at national and EU level to meet the set deadlines. This was perceived both as a challenge – especially for Member States relying on limited resources in this area – and as an opportunity to set up new cooperation mechanisms, and to develop activities and expertise in this field.

The various steps and deliverables of the Recommendation, including the risk assessment phase and ensuing Toolbox measures, were perceived as bringing significant added value to Member States. The Recommendation process and ensuing Toolbox also had the effect of raising the profile of the issue of 5G cybersecurity and bringing it higher on national political agendas. It helped mobilise expertise and create or deepen cooperation mechanisms between the various responsible authorities (e.g. cybersecurity authorities, telecoms regulators, Ministries of Digital Affairs, Home Affairs, Defence, Justice, Trade, Economy, etc.), and also with the private sector, in particular mobile operators and their suppliers. Besides, some Member States reported that the process itself had a direct impact on the strategies and security-related decisions of mobile networks operators in their country.

At EU level, the process to develop the EU Coordinated risk assessment and the Toolbox was considered well-structured. Member State authorities mainly worked together within a dedicated Work Stream of the NIS Cooperation Group, with the support of the Commission and ENISA. The Work Stream met 14 times between April 2019 and November 2020, which allowed very regular information exchange and close coordination in preparing the deliverables. It also facilitated trust building among Member States, the Commission and ENISA – an essential factor on this sensitive matter. During the risk assessment phase, in each Member State, national authorities analysed their own situation, and performed an analysis of risks and existing mitigations/gaps and shared the results with the other Member States, the Commission and ENISA. This pooling of expertise allowed for developing a comprehensive and common understanding of the main risks and risk areas. The Toolbox's mitigation measures enabled Member States to develop and coordinate their implementing measures through a comprehensive approach to reinforcing the security of networks.

Finally, it was noted that a strategic outlook on this issue should continue to account for international developments and that it is key to consolidate a common EU voice and vision towards third country partners. Moreover, the urgency of the issue is calling for a rapid response that should be anchored in a long-term and comprehensive approach, looking at the entire 5G value chain and ecosystem and preparing the ground for future network generations.

2. The EU Toolbox

2.1. The Toolbox measures

Based on the findings of the risk assessments at national and at EU level, the EU Member States, with the support of the Commission and ENISA, worked to develop a Toolbox of mitigating measures. Measures identified in the Toolbox include Strategic and Technical measures. The Toolbox preparation also received targeted input from BEREC.

Strategic measures (SM) cover measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities, as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic and long-term dependency risks. Technical measures (TM) include actions to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors.

A set of Supporting actions is included to complement and enhance the effectiveness of the Strategic and Technical measures (e.g. cybersecurity cooperation, Telecoms Code, standardisation, certification, Foreign Direct Investment (FDI) screening, trade defence instruments, competition rules, EU funding, public procurement rules, industrial development and deployment).

Based on the assessment of possible risk mitigation plans and the identification of the highest effectiveness measures, the 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."*

2.2. Implementation of the Toolbox measures by Member States

On 22 July 2020, the NIS Cooperation Group published a Progress report[18], which analyses the implementation of key Toolbox measures as of June 2020, and looks at the nature of the national measures adopted or planned. The report also provides an initial assessment of the degree of convergence of adopted and planned measures, as well as possible gaps and areas where further action is needed.

This Progress report showed that – while work is still ongoing in many Member States – overall, good progress has been made in implementing the Toolbox measures and all Member States reported that concrete steps have been taken. This demonstrates a strong commitment by Member States to the coordinated approach defined at EU level. For certain measures in particular, the report highlighted that particular attention or more efforts are needed in the next phase of the implementation process.

Specifically, the Progress report of July 2020 concluded that good progress had already been achieved for some of the Toolbox measures, namely in the following areas:

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

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

[18] Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, 24 July 2020, https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

government or other critical entities. For those operators having already contracted with a high-risk suppliers, transition periods for switching to more secure suppliers should be put in place.

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

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

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

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

- On FDI screening, steps should be taken to introduce national FDI screening mechanisms without delay in 13 Member States where it is not yet in place, including in view of the application of the EU investment screening framework as of October 2020. These screening mechanisms should be applied to investment developments potentially affecting the 5G value chain, taking into account the objectives of the Toolbox.

Following this report and based on the information gathered during bilateral meetings with Member States organised by the Commission with the support of ENISA, it can be concluded that Member States have made further progress in implementing the various measures at national level, with a very large majority indicating clear plans and timelines for the roll-out of the measures recommended in the Toolbox conclusions. Nearly all Member States estimate that they will complete the ongoing national implementation processes by mid-2021.

However, there are some differences between individual measures, with some Member States being more advanced in certain areas than in others. Overall, **this review confirmed that, as regards areas where more efforts and particular attention is needed, the assessment and conclusions of the Progress report remain entirely valid.**

At the same time, since the technology and threats are continuously evolving, parts of the national frameworks will need to be kept up-to-date. Consequently, many Member States intend to maintain a structured process in order to be able to adjust certain aspects of their measures, in light of future developments.

Strategic measures - main developments since the Progress report of July 2020

A large majority of Member States have adopted or are at a final stage of adopting the legal framework to strengthen the **regulatory powers of national authorities** to be able to impose

strengthened obligations on operators and to impose restrictions or to prohibit the supply, deployment and operation of 5G network equipment (SM01)[19].

As regards **high-risk suppliers**, as of November 2020, measures aimed at applying restrictions based on the risk profile of suppliers have been adopted, proposed or planned in nearly all Member States, taking into account the approach recommended in the Toolbox. Only a small minority of Member States have yet to define clear plans to implement these measures.

This reflects the high degree of priority given to the risks that these measures are intended to address in the national risk assessments (risk of lack of access controls and risk of interference by a State actor). This also reflects the strong commitment by Member States in this area, as reiterated by the European Council on 2 October 2020, which called on Member States *"to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments, based on common objective criteria"*[20].

As a consequence, the reliance on high-risk suppliers, which is currently estimated by many Member States as medium to high, is expected to decrease in the coming year(s) as 5G network roll-outs progress, albeit with variations between individual Member States, depending on the initial level of exposure (especially where network operators had already entered into 5G contracts with high-risk suppliers before the adoption of the Toolbox), on the scope of the restrictions imposed and on the timeframe for switching to more secure suppliers.

The Toolbox and EU Coordinated risk assessment provide guidance on the objective criteria that are to be used for assessing the risk profile of suppliers and on key assets considered critical and sensitive. As part of the next steps for the work at EU level, Member States confirmed their strong interest in continuing the cooperation and exchange of information on how best to tackle risks emanating from high-risk suppliers. Work has already been done within the NIS Cooperation Group to deepen the common understanding of the practical implementation of the guidance laid down in the Toolbox, notably through two workshops among national authorities on this topic.

On **suppliers' diversification and resilience** (SM05 and SM06)[21], several Member States have introduced measures, such as requesting that MNOs submit their sourcing and diversification strategies to national authorities and ensure that they take measures to increase resilience. Other Member States have not yet taken specific measures due to several challenges already identified in the July Progress report (e.g. size of the country, difficulties to define appropriate multi-vendor strategies, interoperability issues). Many Member States are calling for further exchanges at EU-level and for exploring possible practical guidance for national approaches.

On this topic, BEREC conducted a survey looking in more detail into the state of implementation of SM05 and SM06 and providing a snapshot of the current suppliers' base of MNOs in the EU and their multi-vendor approaches. In addition, BEREC also organised

[19] SM01: Strengthening the role of national authorities.
[20] EUCO 13/20, Special meeting of the European Council (1 and 2 October 2020) – Conclusions.
[21] SM05: Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies – SM06: Strengthening the resilience at national level.

webinars with suppliers and with operators' associations to gather their views on these two Strategic measures.

As a result of this survey, BEREC has identified the need to establish a greater understanding of several issues, in particular as regards: (1) specific risk scenarios related to the 5G supply chain (e.g. risks related to the MNOs' full supply chain, including in case of disruption in the supply market), (2) potential gains and limitations of network architectures such as Open RAN, i.e. more open and interoperable interfaces in Radio Access Networks (RAN), including the likely timeline before they can become a viable approach; and (3) a more holistic understanding of the costs and impacts related to implementing various approaches of multi-vendor strategies by MNOs.

As regards Strategic Measure 07 **(Foreign Direct Investment screening),** there are now 15 Member States which have national screening mechanisms in place. In addition, several other Member States have indicated that a process to develop a FDI screening system is underway. The EU framework for the screening of FDI became fully operational as of 11 October 2020. EU rules provide a framework to ensure the protection of legitimate public policy objectives if such objectives are threatened by foreign investments. The EU Regulation lays down a number of factors and considerations that are relevant to determine whether a Foreign Direct Investment is likely to affect security or public order. In its Communication of 13 March 2020[22], the Commission indicated that the Member States *"need to be vigilant and use all tools available at Union and national level to avoid that the current crisis leads to a loss of critical assets and technology"* which are crucial to Europe's security, and are part of the backbone of its economy.

Technical measures - main developments since the Progress report of July 2020

A majority of Member States has made good progress in implementing the Technical measures of the Toolbox. Most Member States have put in place concrete activities and have a clear vision and specific plans on strengthening requirements for MNOs in line with the Toolbox Technical measures. Nonetheless, a few Member States indicated having no concrete plans for either strengthening the baseline security requirements or for introducing any new 5G specific measures at this stage. In almost half of the Member States, changes and reinforcements to their current security framework are under development or are already implemented. These changes are mostly driven by the process of transposing the European Electronic Communications Code and are therefore typically targeting baseline measures in a technology-neutral way. A certain number of Member States are adding specific reinforcements for 5G and a few Member States will consider new 5G-specific measures at a later stage (e.g. when deployments move to 5G stand-alone, when 5G will be fully virtualised, etc.). A minority of Member States considers their current measures as sufficient or has no plans for changes.

A majority of Member States values ENISA's technical guidelines on cybersecurity measures for telecom security regulatory authorities[23] and uses them for inspiration to establish their own guidelines. In some cases, ENISA guidelines are used directly as a basis for national soft-law or legal instruments for security requirements for operators and/or for audit guidance.

[22] Coordinated economic response to the COVID-19 Outbreak, COM(2020) 112 final.

[23] ENISA Technical Guideline on Minimum Security Measures, 24 October 2014, https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures

This year, ENISA, together with the Article 13a Expert Group produced new, updated guidelines[24]. It includes alignment with the European Electronic Communications Code and general, technology-neutral reinforcements of a number of security objectives aligned with proposed reinforcements in the Toolbox. In addition, a 5G supplement[25] to these guidelines has been developed in consultation with the NIS 5G Work Stream and the Article 13a Expert Group, containing additional checklists and additional guidance for national regulatory authorities (NRAs) supervising 5G operators.

ENISA also published an updated Threat Landscape for 5G networks[26] and organised a series of knowledge building webinars focused on technical aspects of 5G security for cybersecurity authorities and members of the NIS 5G Work Stream.

Member States confirmed that challenges and/or slower progress mainly remains in those domains where the July Progress report has also indicated a lack of maturity (e.g. TM08 - Raising the security standards in suppliers' processes through robust procurement conditions, TM02 - Ensuring and evaluating the implementation of security measures in existing 5G standards and/or TM04 - Increasing the security of virtualised network functions). In addition, several Member States have highlighted the challenges related to the implementation of the requirement contained in TM05 - Ensuring secure 5G network management, operation and monitoring, related to location for the establishment of Network Operations Centres (NOC)/Security Operation Centres (SOC). Several Member States have emphasised the importance of further information sharing, collaboration and guidance in technical matters pertaining to these measures.

3. Toolbox supporting actions and other EU-level actions

3.1. Standardisation and certification

As envisaged in Supporting Action 03[27], a Subgroup on 5G standardisation was set up under the NIS 5G Work Stream shortly after the publication of the Toolbox. The Subgroup aims to facilitate coordination between Member States in the areas of 5G standardisation, avoid duplication of national approaches, and promote more secure products and processes as laid down in the conclusions of the Toolbox.

The Subgroup produced a mapping of the existing standards, technical specifications and certification schemes against the risks identified in the EU Coordinated risk assessment.

It also provided a forum to discuss activities related to the development of certification schemes for 5G networks (TM09)[28]. According to the Toolbox's recommended risk

[24] ENISA Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security/
[25] ENISA 5G Supplement to the Technical Guideline on Security Measures Under the EECC report, 10 December 2020, https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security/
[26] ENISA Threat landscape for 5G networks - Updated threat assessment for the fifth generation of mobile telecommunications networks, 14 December 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/
[27] SA03: Supporting and shaping 5G standardisation.
[28] TM09: Using EU certification for 5G network components, customer equipment and/or suppliers' processes.

mitigation plans, while certification is not suitable to address all risks identified in the EU Coordinated risk assessment, in particular risks related to non-technical vulnerabilities, it can play a role in mitigating certain risks, in combination with other measures. On 27 November 2020, the members of the NIS Work Stream on 5G security expressed support for the preparation of a candidate certification scheme related to 5G components and suppliers' processes. Consequently, the Commission is preparing a request in that sense to ENISA, in line with Article 48 of the Cybersecurity Act.

Furthermore, the Toolbox also refers to the relevance of non-5G specific cybersecurity certification schemes for ICT products and services, such as cloud services and connected (end-user) devices, including Internet of Things. In this respect, it is worth noting that ENISA is currently working on a candidate scheme for cloud services and that in recent Council Conclusions[29], the Council invited the Commission to consider cybersecurity certification for connected devices in the Union Rolling Work Programme for Cybersecurity certification that is currently being developed.

Moreover, to provide further guidance to Member States regarding standardisation, ENISA is drafting a report containing recommendations for the implementation of security measures in existing 5G standards. This report is currently being finalised in consultation with Member States and should be published in early 2021.

3.2. Investments in EU capacities in the area of network technologies

The Commission proposed as a candidate partnership the Smart Networks and Services (SNS) Joint Undertaking, as part of a set of nine proposed Joint Undertakings under Horizon Europe[30]. The objective of this Joint Undertaking would be to enable the EU to develop next generation network technologies and put on the market European solutions that are competitive, enrich the globally available alternatives and diversify the sources of supply, in line with the EU industrial strategy and the Toolbox. It is expected to be launched in Q3 2021, after adoption by the Council.

The proposed Joint Undertaking will have two pillars and will coordinate research activities on 6G technology under Horizon Europe as well as 5G deployment projects under the Connecting Europe Facility Digital and other deployment programmes.

Supported activities under its first pillar will aim at fostering Europe's technology sovereignty in 6G by implementing the related research and innovation (R&I) programme leading to conception and standardisation around 2025, as well as validation and preparation for early market adoption of 6G technologies by the end of the decade. Mobilising a broad set of stakeholders will be key to address strategic areas of the networks and services value chain from edge- and cloud-based service provisioning to market opportunities in new components and devices beyond smartphones.

R&I initiatives on 6G technologies are now starting in leading regions world-wide, with the first products and infrastructures expected for the end of this decade. Europe needs to

[29] 13629/20, Council Conclusions on the cybersecurity of connected devices, 2 December 2020, https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf

[30] https://ec.europa.eu/info/sites/info/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_orientations-he-strategic-plan_122019.pdf

position itself to ensure the best outcome both for the digital economy at large, but also for the technology capabilities of our existing and emerging industrial players. This calls for a strategic partnership with a solid R&I roadmap set out and followed by a critical mass of European actors. The EU supply chain will be strengthened by investing in key connectivity projects to develop and deploy strategic industrial capacities and infrastructure. These concern new business models and players through software networks with architectures such as Open RAN and the convergence with new technologies in the area of cloud and edge computing, as well as artificial intelligence.

As an immediate action to foster a diverse and sustainable 5G ecosystem in the EU, the Commission has been facilitating R&I in the area of software-based networks, including Open RAN. Nine innovation actions in this field have been selected under a recent Horizon 2020 call[31] and are expected to kick off in January 2021. The aim is not only to foster supply diversity and reduce costs, but also to enable innovative 5G services for consumers, businesses and vertical industries.

The Commission is planning to continue these activities under the upcoming funding programmes. R&I actions can be funded under the proposed Smart Networks and Services Joint Undertaking, whereas pilot and deployment actions can be funded under the Digital Europe Programme, Connecting Europe Facility and national initiatives under the Recovery and Resilience Facility.

As regards the cybersecurity aspects, Member States authorities have been discussing Open RAN, in particular its potential to increase supply diversity, notably in the context of the survey conducted by BEREC mentioned above and within the NIS Work Stream. These discussions highlighted the need to establish a greater understanding of the potential gains and limitations of Open RAN also from the perspective of security.

For this purpose, the Commission has recently launched an independent study to identify existing and expected market trends and identify possible policy measures for European and national authorities to address the risks and opportunities in the field of Open RAN[32].

3.3. EU funding for secure 5G deployment

Building on the Toolbox Supporting Action 10[33], the Commission announced in its Communication 'Secure 5G deployment in the EU - Implementing the EU Toolbox' that it will ensure that participation in relevant technology domains will be conditional on compliance with security requirements, by making full use of and further implementing security conditions in R&I programmes, in particular in Horizon Europe, the Digital Europe Programme and Connecting Europe Facility 2, in European structural and investment funds and in other relevant programmes[34]. A similar approach will also be taken in the EU's external funding programmes and financial instruments, including on funding provided

[31] Call ICT-52-2020 Smart Connectivity Beyond 5G Horizon 2020.

[32] https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-study-5g-supply-markets-and-open-ran

[33] SA10: Ensuring 5G projects supported with public funding take into account cybersecurity risks.

[34] The budgetary impact of the EU funding mentioned under section 3.3 'EU funding for secure 5G deployment' will be entirely covered by the allocations foreseen in the Multiannual Financial Framework 2021-2027 under the financial envelopes of the affected programmes.

through international financial institutions. To implement this approach, the Commission is currently working to introduce cybersecurity requirements that are in line with the Toolbox in the relevant Work programmes and Calls for proposals.

In particular, the second pillar of the proposed Smart Networks and Services Joint Undertaking aims at boosting 5G deployment in Europe in view of developing digital lead markets and of enabling the digital and green transition of the economy and society. For this objective, possible actions include the coordination of strategic guidance for the relevant programmes under the Connecting Europe Facility, in particular 5G Corridors, as well as other European programmes and facilities such as the Digital Europe Programme, InvestEU and national programmes. In this context, the Commission aims to ensure that Work Programmes or Calls for proposals under the Smart Networks and Services Joint Undertaking will require actions to follow security scrutiny assessments and will apply appropriate eligibility criteria in piloting and deployment actions in line with the Toolbox.

Additionally, accelerating 5G deployment is a priority area for funding under the Recovery and Resilience Facility (RRF). To guide the implementation of the RRF projects supporting the digital transition, the Commission has issued general guidance[35] that encourages Member States to use their recovery plans to inter-alia focus investments on secure connectivity and on the expansion of very high capacity networks including 5G and fibre in line with the 2025 connectivity objectives, taking into account the Toolbox. Funding under the RRF is subject to State aid rules.

3.4. International activities

The Toolbox and its risk-based objective process has triggered a strong interest from a wide range of stakeholders from outside the European Union. Member States representatives, as well as representatives of the Commission and of ENISA have participated in numerous events, including multilateral and bilateral exchanges, where they presented the Toolbox and its comprehensive, objective and risk-based approach. The Commission services, together with the European External Action Service, are also actively monitoring relevant developments in third countries through the EU network of Delegations.

Moreover, the Toolbox has become an important element in the EU's strategic dialogues and partnerships with third countries. Indeed, the Commission services together with the European External Action Service, are working to ensure that EU strategic interests are protected in third countries through existing policy dialogues with partner countries and through the possible development of other strategic alliances in order to lead the digital global governance in the field of 5G cybersecurity, in accordance with EU standards and values.

Third countries have shown a strong interest for the process followed at EU level and the resulting Toolbox of mitigation measures, which has been developed following a risk-based and objective approach. While the Toolbox has been drawn up mostly with the view to provide guidance to EU Member States, similar measures could certainly be of relevance in other countries when designing or implementing their policy and regulations on 5G

[35] Recovery and Resilience Plans - Example of component of reforms and investments 'Digital connectivity' https://ec.europa.eu/info/sites/info/files/component_digital_connectivity.pdf

cybersecurity. The Toolbox indeed provides a methodology that other countries can use to assess and prioritise risks and to define comprehensive and effective mitigation approaches.

Conclusions

This review shows that Member States remain strongly committed to the EU coordinated process on 5G cybersecurity based on the Commission Recommendation. It confirms that the Toolbox enables a common EU approach to 5G cybersecurity, which is risk-based and objective, and supports consistency across the internal market through EU policies and coordination, as well as the exercise of Member States' competences, notably in national security.

Member States consider the Toolbox as an effective instrument, providing useful and comprehensive guidance for developing national measures and covering key issues, through a clear and efficient methodology on 5G cybersecurity and is allowing Member States to take actions that fit into a broader framework at EU level.

As shown in the Progress report published in July 2020 by the NIS Cooperation Group, all Member States are in the process of putting in place measures to reinforce the cybersecurity of 5G networks. Since the Progress report was published, most Member States have made further progress in implementing the measures recommended in the Toolbox conclusions at national level, albeit with some differences in pace and depending on the measures. While the national processes are still underway, they are well on track to be completed in the coming months in most Member States. However, as demonstrated in the July Progress report, a number of areas require specific attention and there are still a few Member States were no clear plans have yet been communicated as regards certain measures.

Member States indicated the wish to proceed with the EU coordinated approach developed as a result of the Commission Recommendation, notably by **continuing the work in the NIS Cooperation Group** and **building on it to promote further convergence** in national approaches using existing structures and cooperation channels.

Based on the above findings and consultations with Member States, key objectives and concrete actions for the next steps of the coordinated work at EU level are set out in an Appendix to the EU's Cybersecurity Strategy for the Digital Decade[36].

[36] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18.