Council of the
European Union

Brussels, 30 January 2020
(OR. en)

5664/20

TELECOM 9
CYBER 12
COMPET 20
MI 16
CONSOM 13

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	30 January 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2020) 50 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Secure 5G deployment in the EU - Implementing the EU toolbox

Delegations will find attached document COM(2020) 50 final.

Encl.: COM(2020) 50 final

EUROPEAN
COMMISSION

Brussels, 29.1.2020
COM(2020) 50 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Secure 5G deployment in the EU - Implementing the EU toolbox

1. *Introduction*

The fifth generation (5G) of telecommunication networks are set to play an essential role in the development of the European society and economy. They are 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 will therefore potentially impact close to all aspects of the lives of EU citizens. The cybersecurity of 5G networks is therefore essential not only to protect our economies, societies and democratic processes but also to ensure a trustful digital transformation for the benefit of all EU citizens.

The dependence of many critical services on 5G networks would make the consequences of systemic and widespread disruption particularly serious and, given the interconnected nature of the digital ecosystems, could have significant impacts beyond national borders. As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union, at a time when cyber-attacks are on the rise, more sophisticated than ever and coming from a wide range of threat actors, in particular non-EU state or state-backed actors. Regarding the security of critical infrastructures as 5G, the approach chosen is to define, for the first time, a common European approach. This approach is in full respect of the openness of the EU internal market as long as the risk - based EU security requirements are respected.

The European Council on 22 March 2019 called for a concerted approach to the security of 5G networks. On 26 March 2019, the Commission adopted a Recommendation (EU) 2019/534 on the cybersecurity of 5G networks[1]. 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. This Communication forms an integral part of the Commission's comprehensive European digital strategy, as called for by the European Council.

2. *5G roll-out in the EU*

The deployment in Europe of 5G network infrastructure is central for the European industrial strategy and competitiveness. The Commission has recognised 5G deployment of network technologies as a major enabler for future digital services. In 2016, the Commission adopted the 5G Action Plan to make sure that the Union has the connectivity infrastructure necessary for its digital transformation as of 2020 and for comprehensive deployment in urban areas and major transport paths by 2025[2]. The Gigabit Society Communication sets the ambition that there should be access to mobile data connectivity everywhere[3], including in rural and remote areas.

As regards the assignment of frequencies, Member States have assigned 16% of the 5G pioneer bands[4]. Consultations for a number of assignment procedures are expected in the next

[1] Recommendation (EU) 2019/534 on the cybersecurity of 5G networks, OJ L 88, 29.3.2019, p. 42–47.
[2] COM(2016) 588 of 14 June, 2016 on 5G for Europe: An Action Plan.
[3] COM(2016)587 "Connectivity for a Competitive Digital Single Market – towards a European Gigabit Society".
[4] http://www.5GObservatory.eu

few months in view of the legal obligation to allow the use of all 5G pioneer bands by the end of the year.

Europe is one of the most advanced regions in the world as regards the commercial launch of 5G services[5]. Currently, first 5G services are expected to be available in 138 European cities by the end of 2020. Early 5G networks build on the current 4th generation (4G) of network technologies and 5G services are mainly provided for the general public, either as an improvement to 4G in terms of capacity and speed, or as a cost-effective wireless alternative to fixed networks[6].

As regards opportunities in new business-to-business services, such as in the energy, food and agriculture, healthcare, manufacturing or transport sectors, Europe is well advanced with an investment in the order of €1 billion, including €300 million of EU funding in the context of the 5G Public Private Partnership under Horizon 2020. This investment includes more than 160 large-scale 5G trials identified in Europe, including ten cross-border highway corridors for large-scale testing of 5G-based Connected and Automated Mobility services. Trials include 5G-enabled applications in areas spanning from sustainable healthcare and automated mobility resource-efficient agriculture to smart electricity networks and Industry 4.0. In addition to this, the EIB supported by the European Fund for Strategic Investment, provided loans to accelerate research and development of 5G technology.

The European Electronic Communications Code ('The Code')[7] that will apply from 21 December 2020 is an important basis to create an investment friendly environment for 5G networks and beyond. Furthermore, public funding programmes, such as the Connecting Europe Facility Digital[8] or European structural and investment funds will also be essential to support future deployment of 5G networks, in particular by connecting communities to 5G-enabled services like schools, hospitals, cities and local administrations.

Considering Europe's strategic opportunities in 5G services for various industries, it will be of paramount importance that operators and service providers invest in advanced 5G network and service solutions. These will not only require new 5G radio networks but also new so-called 'stand-alone' 5G core networks, in order to provide advanced 5G functionalities like network slicing[9] and edge computing[10].

The Commission will continue to fully support the successful 5G roll-out in the EU, including by engaging with Member States and stakeholders to seize the opportunities of 5G. Due

---

[5] http://www.5GObservatory.eu

[6] Some of the new functionalities of 5G will be introduced following a phased approach. In a first phase (very short or short-term), 5G deployment will consist primarily in 'non stand-alone' networks, where only the radio access network is upgraded to 5G technology, and otherwise still relies on existing 4G core networks, which will provide enhanced mobile broadband performances to end-users. During subsequent phases (short/mid-term to long-term), deployment of 'stand-alone' 5G networks, including 5G core network functions, will require and will result over time in a much more extensive change in the network architecture.

[7] Directive (EU) 2018/1972 of the European Parliament and the Council establishing the European Electronic Communications Code (Recast).

[8] Proposal for a Regulation COM(2018)438 of 6 June, 2018 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014

[9] 5G network slicing allows a high degree of separation between different service layers on the same physical network, thus increasing the possibilities to offer differentiated services over the whole network.

[10] Edge computing is a distributed computing paradigm which brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth.

consideration will be given to relevant health aspects based on the precautionary principle[11], in cooperation with relevant international organisations and the scientific community.

3. The EU Coordinated Risk Assessment on Cybersecurity in 5G Networks

Working collectively within the NIS[12] Cooperation Group, 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, by early July 2019.

Based on these national risk assessments, on 9 October 2019the NIS Cooperation Group, formed of representatives of Member States, the Commission and ENISA, published a report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks[13]. The report identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) affecting 5G networks. On this basis, the report also identified a number of categories of risks of strategic importance from an EU perspective illustrated by concrete risk scenarios, which reflect relevant combinations of the different parameters (vulnerabilities, threats and threat actors) with respect to the different assets (see Appendix).

To complement this report and as a further input for the toolbox, ENISA carried out a dedicated threat landscape mapping[14], consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting these.

The EU coordinated risk assessment report highlights a number of aspects of importance for 5G networks. Specifically:

a) The technological changes introduced by 5G will increase the overall attack surface and the number of potential entry points for attackers:

- Enhanced functionality at the edge of the network and a less centralised architecture than in previous generations of mobile networks means that some functions of the core networks may be integrated in other parts of the networks making the corresponding equipment more sensitive (e.g. base stations or MANO functions);

-The increased part of software in 5G equipment leads to increased risks linked to software development and update processes, creates new risks of configuration errors, and gives a more important role in the security analysis to the choices made by each mobile network operator in the deployment phase of the network;

b) These new technological features will give greater significance to the reliance of mobile network operators on third-party suppliers and to their role in the 5G supply chain.

[11] Council Recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC).

[12] 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 (NIS Directive). The NIS Cooperation Group has been established by the NIS Directive to ensure strategic cooperation and the exchange of information among EU Member States in cybersecurity.

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

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

This will, in turn, increase the number of attack paths that could be exploited by threat actors, in particular non-EU state or state-backed actors, because of their capabilities (intent and resources) to perform attacks against EU Member States telecommunications networks, as well as the potential severity of the impact of such attacks.

In this context of increased exposure to attacks facilitated by third-party suppliers, the individual risk profile of suppliers will become particularly important, in particular where a supplier has a significant presence within networks or areas.

c) A major dependency on a single supplier increases the exposure to and consequences of a potential failure of this supplier. It also aggravates the potential consequences 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.

d) If some of the new use cases envisioned for 5G come to fruition, 5G networks will end up being an important part of the supply chain of many critical IT applications, and as such not only confidentiality and privacy requirements will be impacted, but also the integrity and availability of those networks will become major national security concerns and a major security challenge from an EU perspective.

Source: EU coordinated risk assessment

The EU coordinated risk assessment 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 5G sector and its ecosystem, and making it essential for Member States to take the necessary mitigating measures.

To address the identified risks effectively and strengthen the security and resilience of 5G networks a comprehensive approach is required which implies putting in place a set of key measures as well as related supporting actions which can address the risks at the same time. The EU coordinated risk assessment provided the basis to identify mitigation measures that can be applied at national and European level.

The Council Conclusions of 3 December 2019 supported the findings of the coordinated risk assessment and stressed 'the importance of a coordinated approach and effective implementation of the Recommendation in order to avoid fragmentation in the Single Market'[15]. 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.'

[15] 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.

4. The EU toolbox on 5G cybersecurity

On 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk mitigating measures[16]. It addresses all the risks identified in the coordinated risk assessment report.

The EU toolbox identifies and describes a set of strategic and technical measures, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place in order to mitigate the identified risks. **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, 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. **Technical measures** include measures to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors. Moreover, for each of the risk areas identified in the EU coordinated risk assessment, it provides for **risk mitigation plans** based on the highest effectiveness measures.

Among them, the conclusions of the EU toolbox, as agreed by the NIS Cooperation Group, recommends a set of **key measures** to be implemented by all Member States and by the Commission, as follows:

Conclusions of the EU toolbox

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*

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

(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:*

  *o 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*

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

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

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.***

Source: EU toolbox.

The toolbox conclusions demonstrate the strong resolve of Member States to jointly respond to the security challenges of 5G networks. This is of fundamental importance for security within Member States and EU-wide, for national economies as well as for the EU internal market and Europe's technological sovereignty. Both the EU coordinated risk assessment and

the EU toolbox show the high value of the collective work done in the NIS Cooperation Group, with the intensive collaboration between representatives from all Member States, the Commission and ENISA.

The toolbox enables a common EU approach to 5G cybersecurity, supporting consistency across the internal market through EU policies and coordination, as well as the exercise of Member States' competences notably regarding national security. The mitigating measures and mitigation plans it contains allow for an appropriate, effective and proportionate EU response to common 5G cybersecurity challenges.

The Commission welcomes the publication of the EU toolbox on 5G cybersecurity and fully supports all its above conclusions.

The Commission calls on Member States and relevant Union institutions, agencies and other bodies to:

(i) ensure the swift implementation of effective and appropriate risk mitigating strategies across the EU in line with the EU toolbox, and

(ii) take all necessary further steps to ensure coordination at Union level, including through continued work within the NIS Cooperation Group and setting up a robust mechanism to monitor the implementation of the EU toolbox, in order to ensure the effectiveness of the measures and the smooth functioning of the internal market.

5. Implementing the toolbox

The determination of Member States in making full use of the toolbox is essential for a credible and successful European approach to 5G security. While Member States will decide on the suitability of a particular measure based on national circumstances, it is absolutely essential that a **set of key measures, as recommended by the NIS Cooperation Group (see toolbox conclusions above), is put in place in every Member State and, for some of the measures, at EU level,** in order to address the risks that have been identified.

The Commission is ready to continue to provide its full support during the next phases and calls on Member States:

- **by 30 April 2020,** to take concrete and measurable steps to implement the set of key measures recommended in the EU toolbox conclusions;

- **by 30 June 2020,** to prepare a report by the NIS Cooperation Group on the state of implementation in each Member States of these key measures , based on the regular reporting and monitoring carried out notably within the NIS Cooperation Group, with the support of the Commission and ENISA.

5.1. A risk-based, concerted approach to 5G suppliers

Given the ultimate objective to ensure the security and resilience of the 5G networks and their sustainability, Member States agreed on the need to assess the risk profile of individual suppliers and, as a consequence to apply relevant restrictions for suppliers considered to be high risk, including necessary exclusions to effectively mitigate risks, for key assets, as

indicated in the toolbox. The Commission is ready to support the Member States in implementing these measures.

To support their implementation across the EU, the EU coordinated risk assessment and the EU toolbox provide guidance regarding (1) the assessment of the risk profile of suppliers[17] and (2) the sensitivity of network elements and functions[18], as well as other assets. Both the EU coordinated risk assessment and the toolbox measures cover the risks related to the suppliers of 5G network equipment and network services. They do not cover the other products or services that these or other suppliers may provide.

As defined in paragraph 2.37 of the EU coordinated risk assessment, the risk profiles of individual suppliers can be assessed on the basis of several factors.

The assessment of the risk profiles of suppliers should be conducted solely on security grounds and based on objective criteria. In order to facilitate a coordinated approach on the implementation of these measures, the toolbox recommends that Member States exchange information about national approaches and best practices. Furthermore, it is the Commission's view that this action should be one of the first priorities of the next phase of the work within the NIS Cooperation Group, together with the Commission and ENISA.

It is important that restrictions concerning suppliers considered to be high risk, including necessary exclusions to effectively mitigate risks, as well as measures to avoid dependency on these suppliers, are taken in a timely manner. Doing so at the earliest stage, including where possible in relation to the 5G frequencies licensing processes, will also increase predictability for market operators, thereby contributing to a swift roll-out of 5G networks, and will ensure the long-term security of 5G networks and resilience of the 5G supply chain.

At the same time, the national implementation of these measures may specify different timeframes, where necessary and justified, in particular in case of a high degree of existing reliance on equipment or services from suppliers assessed to be high risk (e.g. by taking into account equipment upgrade cycles, in particular the migration from 'non stand-alone' to 'stand-alone' 5G networks). Member States could consider defining implementation plans that might include appropriate transition periods for concerned network operators. In this context, transition periods should be defined in such a manner as to preserve or even strengthen incentives to invest in modern network equipment, including accelerating the deployment of fully-fledged ('stand-alone') 5G core networks and replacing existing 4G equipment in other parts of the networks (e.g. in the Radio Access Network), in line with the objectives of the 5G Action Plan.[19]

Additionally, due to the complexity of the 5G software-based networks, telecom operators may increasingly rely on third party entities to perform certain tasks, such as the maintenance and upgrade of the 5G networks and software, as well as other outsourced managed services, in addition to the supply of network equipment. As described in the EU coordinated risk assessment, this constitutes a source of serious security risk. Particular attention should

[17] Paragraph 2.37 of the EU coordinated risk assessment.

[18] Paragraph 2.21 of the EU coordinated risk assessment presents the main categories of elements and functions and their overall level of sensitivity, and lists a number of key elements identified by Member States for each category and paragraphs 2.28 and 2.29 identify a number of other types of sensitive assets or areas (e.g. specific entities or geographic areas).

[19] COM(2016)588 of the 14 September, 2016 5G for Europe: An Action Plan.

therefore be paid to this aspect. It is essential that a thorough security assessment is also done of the risk profile of the suppliers tasked with these services, in particular when these tasks are not performed in the EU. Appropriate measures should be taken, including applying restrictions in particular in sensitive parts of the 5G networks or necessary exclusion of high risk entities in line with the mitigating measures of the toolbox, in order to preserve the long-term integrity of the 5G infrastructure.

5.2. The Commission's role in supporting the toolbox implementation

The Commission will continue supporting the implementation of the EU approach on 5G cybersecurity in general, as well as taking specific initiatives in relation to measures and objectives of the toolbox where it can add value. The Commission will make full use of its competences and relevant instruments to the extent necessary to address the identified security considerations. By doing so, and by acting collectively together with Member States and the private sector, the Commission seeks to support strategic measures that will contribute to ensure EU technology sovereignty and leadership in future development of network technologies, in cybersecurity technologies and all relevant building blocks on which our whole economy and security depend.

More specifically, the Commission will undertake the following to ensure implementation of the corresponding mitigating measures in the toolbox in the areas under its competence:

Safeguarding the cybersecurity of 5G networks and a diverse 5G value chain:

-**Cybersecurity cooperation**: Continue to provide support to Member States for the effective, coordinated and timely implementation of national measures through the NIS Cooperation Group.

- Telecoms and cybersecurity rules: Provide support for the implementation of toolbox measures relating to security requirements, notably with regard to relevant provisions under European rules on electronic communications, and consider the added value of possible implementing acts detailing technical and organisational security measures in order to complement national rules and enhance the effectiveness and consistency of security measures imposed on the operators.

- **Standardisation**: Take action to help maintain and where needed increase European participation in the respective standardisation bodies, in order to achieve Europe's security and interoperability objectives. In particular, the Commission will, together with the Member States, assess and promote the technical specifications and standards enabling interoperability between suppliers of 5G equipment in different parts of the network, including in legacy networks, to enable a true multi-vendor environment, through for example open, interoperable interfaces.

- **Certification**: Support the development of 5G certification schemes addressing the needs of 5G networks under the EU's cybersecurity certification framework.

- **Foreign Direct Investment (FDI) screening**: Support the implementation of the EU screening framework by mapping the 5G value chain, including sensitive network assets, and regular monitoring of FDI along the value chain. In line with the FDI screening timeline (as of October 2020), the Commission will scrutinise foreign investments in the 5G area in line with

the guidelines provided in Regulation EU2019/452, taking into account the EU coordinated risk assessment and the EU toolbox.

- Trade defense instruments: Monitor all relevant market developments in the EU and in third countries, and protect EU actors in the European 5G market with trade defense measures to address potential trade distorting practices (dumping or subsidisation), including by launching preliminary enquiries where appropriate.

- Competition rules: Monitor the functioning of the markets for the supply of 5G hardware and software with a view to ensuring that they deliver competitive outcomes, including in relation to possible contractual or technical 'lock-in' situations.

- **EU funding programmes**: Ensure that participation in EU funding programmes 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. A similar approach should also be taken in the EU's external funding programmes and financial instruments, including with regard to funding provided through international financial institutions.

- Public procurement: Leverage public procurements in the area of 5G networks to support identified objectives of security, diversity of suppliers and long-term sustainability of 5G networks; in particular, seek to ensure the due consideration of security aspects in the awarding of public procurement contracts related to the area of 5G networks, in line with the EU public procurement rules.

- Incident response and crisis management (Blueprint) and Cyber exercises: Make full use of the development of the EU's Blueprint[20] on the coordinated response to large-scale cybersecurity incidents. In addition, together with ENISA, consider the possibility of conducting a 5G cyber exercise as soon as the maturity of the market allows.

And, under the responsibility of the High Representative of the Union for Foreign Affairs and Security Policy and Vice President of the Commission, and the Council:

- **Framework for Joint EU Diplomatic response to malicious cyber activities (Cyber Diplomacy toolbox)[21]**: In case of malicious cyber activities that threaten the integrity and security of the EU, Member States are encouraged to use relevant Common Foreign and Security Policy measures part of the EU Cyber Diplomacy Toolbox, (including, if necessary, restrictive measures), to encourage cooperation, facilitate mitigation of threats and influence the behavior of potential aggressors.

Moreover, a number of programmes will contribute to the objectives of avoiding or limiting the risk of long-term dependency, by promoting a diverse and sustainable market for 5G, including by maintaining EU capacities in the 5G value chain and investing in innovation, in line with the EU's international obligations.

[20] Commission Recommendation on a coordinated response to large-scale cybersecurity incidents & crisis (EU 2017/1584).
[21] Council Conclusions 20 November, 2017, 9916/17.

Promoting innovation and investing in cybersecurity and in network infrastructure technologies:

- EU funding **programmes**: Increase the investments in research, innovation and deployment of network technologies and relevant underlying building blocks. The Commission has proposed close to 3 billion Euro of investments in cybersecurity technologies under the next EU budget 2021-27. This includes research and innovation under Horizon Europe and support to cybersecurity capabilities under the Digital Europe Programme. InvestEU can also provide financial support for research and development in the area of 5G as well as support for its deployment.

Moreover, under the next Horizon Europe[22], the Commission has proposed the set-up of an EU institutionalised partnership on NGI/6G ('Smart Networks and Services'), in partnership with industry and coordination with Member States to complete the deployment of 5G and mainly **to prepare for 6G,** the next generation of mobile technology. More than 2.5 billion Euro of EU investments was proposed from the EU budget (2021-27), to be matched by at least 7.5 billion Euro of private investments in this initiative.

- Industrial development and deployment: Evaluate potential market gaps or failures along the 5G value chain, which would justify targeted interventions under the next long-term budget or a possible IPCEI (Important Projects of Common European Interest) on cybersecurity, in line with the suggestions of the IPCEI high-level forum. The decision to design and set up IPCEIs lies in the hands of Member States and companies. The EU rules provide an enabling framework and the Commission stands ready to facilitate the necessary contacts and provide guidance.

[22] Funding can also be provided through the CEF 2.0 and Digital Europe Programme.

6. Conclusion

5G networks are set to deliver an array of opportunities for the European citizens, society and economy. Ensuring the security and resilience of 5G networks is therefore essential. At the same time, cybersecurity threats (including the risk of interference by non-EU state or state-backed actors) are an evolving challenge, which grows in relevance alongside the increased reliance on technology and data. Neglecting cybersecurity would undermine the trust in the development of the digital economy and society and would prevent the EU from reaping the full benefits of it. This requires a correspondingly evolving and strengthened response.

A coordinated and consistent approach to cybersecurity in the EU for critical technologies and networks is essential for the EU to ensure its technological sovereignty, maintaining and developing industrial capacities. The Commission will fully support the implementation of the EU's cybersecurity approach to 5G networks while ensuring that EU markets remain open to products and services that respect the evolving requirements for cybersecurity and trust.

To this end, it is important that the commitment of all stakeholders around 5G security remains high and will require continued collaboration between Member States, the Commission and ENISA.

As an immediate next step, as outlined above, the Commission calls on Member States to take swift action to implement effectively and objectively the measures agreed as part of the toolbox, and to continue to work together, with the support of the Commission and ENISA, to ensure coordination at EU level. In parallel, the Commission will launch all relevant actions within its competence to support the implementation of the toolbox by Member States and to reinforce its impact.

Appendix: Risk categories (source: EU coordinated risk assessment).

	Risk categories
Risk scenarios related to insufficient security measures	*R1: Misconfiguration of networks*
	R2: Lack of access controls
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
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
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
Risk scenarios related to end user devices	*R9: IoT (Internet of Things) exploitation*