#EU4Digital

EU4Digital: supporting digital economy and society in the Eastern Partnership

Implementation of EU toolbox for 5G security

EU best practice report

June 2023

Funded by
the European Union

Table of contents

Disclaimer: The views and opinions expressed in this document are entirely those of the EY-led consortium and do not reflect the official opinion of the European Commission. Neither the European Commission, nor any person acting on the European Commission's behalf may be held responsible for the content of the information contained in the document.

List of acronyms and abbreviations

Abbreviation	Definition
CSIRTs	Computer Security Incident Response Teams
DSP	Digital Service Provider
Eastern partner countries	Armenia, Azerbaijan, Georgia, Republic of Moldova and Ukraine
ENISA	The European Union Agency for Cybersecurity
EU4Digital Facility, EU4Digital	EU4Digital: supporting digital economy and society in the Eastern Partnership – Phase II
FDI	Foreign Direct Investment
HRV	High Risk Vendors
ICT	Information and Communication Technologies
IoT	Internet of Things
MNO	Mobile Network Operator
MS	Member States
MSP	Managed Service Provider
NFV	Network Function Virtualization
NIS	Network and Information Systems
NOC	Network Operation Center
OES	Operators of Essential Service
R	Risk
SOC	Security Operation Center
SEWG	Spectrum Expert Working Group
SM	Strategic Measure
TM	Technical Measure

1. Introduction

1.1. Legal acts regulating 5G security in EU (1/2)

Main Directives regulating security of 5G network in EU

EU telecommunications framework[1]

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

NIS Directive[2]

- It requires MS to cooperate and share information with each other on cybersecurity matters, and to report serious incidents to ENISA
- Member States must identify essential services and ensure their cybersecurity
- OES and DSPs must take appropriate security measures and report cybersecurity incidents

NIS 2 Directive[3]

- NIS 2 aims to update and strengthen the NIS Directive to address new cybersecurity threats
- It expands the scope to cover more digital services, improves incident reporting and cooperation, and enhances supply chain security
- NIS 2 requires all MS to identify operators of essential services and make sure they take appropriate cybersecurity measures

2002/2018

2016

2023

[1] 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

[2] 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. Accessible via the link.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Accessible via the link.

1.1. Legal acts regulating 5G security in EU (2/2)

EU Toolbox for 5G cybersecurity

Recommendation on 5G cybersecurity[4]

- Set out a number of concrete actions at national and Union level to strengthen the cybersecurity of 5G networks
- NIS 1 Cooperation Group obliged to establish a toolbox identifying types of cybersecurity risk and of possible measures to mitigate the risks

2019

EU risk assessment on 5G cybersecurity[5]

- The report recommends a risk-based approach to 5G security, including identifying and assessing risks
- Identifies the main types of threats posed to 5G networks
- Identifies the main threat actors
- Identifies the main assets and their degree of sensitivity
- Identifies the main vulnerabilities
- Identifies the main risks and related scenarios

2019

NIS 2 Directive

- It is a set of measures (Strategic and Technical) published by the EU to ensure the cybersecurity of 5G networks
- Sets out a common approach to mitigate risks associated with 5G networks
- Aims to provide a comprehensive and coordinated approach to 5G network security across the EU

2020

[4] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks. Accessible via the link.

[5] Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks. Accessible via the link.

1.2. Objectives of the EU Toolbox for 5G Security

What is the EU Toolbox for 5G Security about?

The EU Toolbox for 5G Security aims to promote a coordinated and comprehensive approach to ensure the security of 5G networks in the EU. The toolbox provides guidance to Member States, network operators, and other stakeholders on the security risks and potential vulnerabilities of 5G networks, as well as best practices and mitigation measures to address these risks.

The toolbox covers various aspects of 5G network security, such as risk assessment, security requirements, supply chain security, secure deployment, and incident response. By promoting a common understanding of security risks and implementing consistent security measures across the EU, the toolbox aims to enhance the overall security and resilience of 5G networks. This, in turn, helps to safeguard the EU's critical infrastructure and sensitive information from cyber threats.

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

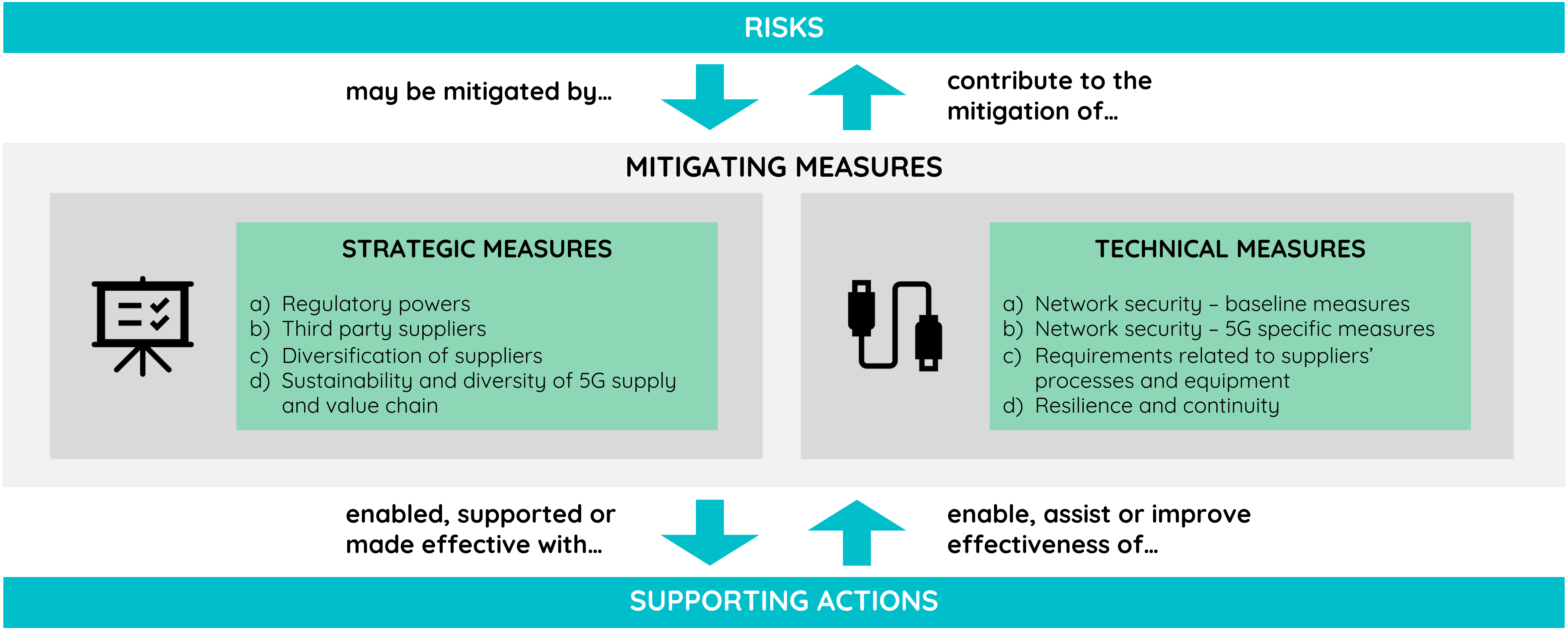
Reasons for introducing regulations

1. The advanced technology of 5G networks, which provides greater speed, capacity, and lower latency, also creates new security challenges, such as increased potential for cyberattacks.
2. Concerns arose regarding third-party vendors, particularly from non-EU countries, participating in the development and deployment of 5G networks, raising issues of supply chain attacks and espionage.
3. The EU considers the secure and resilient 5G network a strategic priority to support its digital transformation. The EU Toolbox for 5G Security aims to provide guidance and best practices to ensure the security and integrity of 5G networks in the EU.

2. Risk mitigating measures

2.1. Scheme of the Cybersecurity risk mitigation

Risk mitigation is possible through implementation of strategic and technical measures



RISKS

may be mitigated by…

contribute to the mitigation of…

MITIGATING MEASURES

STRATEGIC MEASURES

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

TECHNICAL MEASURES

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

enabled, supported or made effective with…

enable, assist or improve effectiveness of…

SUPPORTING ACTIONS

2.2. Risks in 5G networks (1/2)

Main risk categories and example risk scenarios defined by EU coordinated risk assessment

Id	Risk	Risk scenario
a) 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 behavior of the contractor's staff.
b) 5G supply chain		
R3	Low product quality	Intelligence 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 (MNO) 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.

2.2. Risks in 5G networks (2/2)

Main risk categories and example risk scenarios defined by EU coordinated risk assessment

Id	Risk	Risk scenario
c) Modus operandi of main threat actors		
R5	State interference through 5G supply chain	A hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities.
R6	Exploitation of 5G networks by organized crime or Organized 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 MNO itself. Alternatively, using a similar attack path, an organized 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.
d) Dependencies 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 organized crime group.
e) 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 signaling plane.

2.3. Strategic measure - responsible entity

RESPONSIBILITY FOR IMPLEMENTATION

Measures	Relevant actors				
	Member States' Authorities	Mobile Network Operators	European Comission	ENISA	Stakeholders (incl. Suppliers)
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	✓	✓			
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	✓		✓		✓

2.4. List of the strategic measures (1/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
a) Regulatory powers				
SM01	Strengthening the role of national authorities	Strengthen powers for national authorities, to be able to: • impose strengthened obligations on operators, • use ex-ante powers to restrict, prohibit and/or impose specific requirements or conditions	🇪🇪	The Estonian Parliament approved an amendment allowing the government to require communications companies to disclose information about their network hardware and software, and to seek authorization for their use to ensure national security. The details of these obligations and procedures will be determined by secondary legislation
More examples			🇬🇧	The National Cyber Security Centre (NCSC) has been granted regulatory powers to oversee and regulate the security of the country's 5G networks, including imposing obligations on operators and restricting or prohibiting the use of equipment from high-risk vendors
			🇩🇪	The country has established the Federal Office for Information Security (BSI) as the national authority responsible for the security of 5G networks. The BSI has been granted regulatory powers to impose requirements on operators and assess the security of 5G equipment
			🇫🇷	The country has established the National Agency for the Security of Information Systems (ANSSI) as the national authority responsible for the security of 5G networks. ANSSI has been granted regulatory powers to assess the security of 5G equipment and impose obligations on operators to ensure the security of the networks

2.4. List of the strategic measures (2/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
a) Regulatory powers				
SM02	Performing audits on operators and requiring information	• Audit or require audits of MNOs for critical and sensitive parts of 5G networks • Require detailed information from operators about their 5G equipment sourcing and third-party involvement plans • Operators must document how baseline security measures are implemented	🇦🇹	As per the Telecom Network Security Regulation (TNSR), MNOs operating a 5G network must adhere to information security measures, maintain an Information Security Management System (ISMS) according to 3GPP standards, and report 5G network functions and suppliers to the NRA (National Risk Assessment for Austria) biannually
More examples			🇪🇸	The National Cybersecurity Institute (INCIBE) performs audits on 5G operators and requires detailed information about their plans for sourcing 5G equipment and working with third-party suppliers
			🇮🇹	The Ministry of Economic Development performs audits on 5G operators and requires detailed information about their plans for sourcing 5G equipment and working with third-party suppliers
			🇳🇱	The National Cyber Security Centre (NCSC) performs audits on 5G operators and requires detailed information about their plans for sourcing 5G equipment and working with third-party suppliers

2.4. List of the strategic measures (3/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Third party suppliers				
SM03	Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk	• Establish a supplier risk assessment framework with clear criteria • Apply restrictions for critical assets based on rigorous risk assessments • Ensure MNOs have adequate controls to manage residual risks with regular audits and specific supplier requirements	🇮🇹	The Golden Power law requires MNOs to notify the Government when using equipment or services from non-EU suppliers for 5G deployment. An inter-ministerial Coordination Group provides advice to the Government on vetoing contracts or imposing security measures based on technical analysis
		More examples	🇫🇷	The National Agency for the Security of Information Systems (ANSSI) assesses the risk profile of suppliers at the national level and applies necessary restrictions to mitigate risks for critical or sensitive assets
			🇩🇪	The Federal Office for Information Security (BSI) assesses the risk profile of suppliers at the national level and applies necessary restrictions to mitigate risks for critical or sensitive assets
			🇬🇧	The National Cyber Security Centre (NCSC) assesses the risk profile of suppliers at the national level and applies necessary restrictions to mitigate risks for critical or sensitive assets

2.4. List of the strategic measures (4/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Third party suppliers				
SM04	Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support	• Establish legal framework for outsourcing functions to MSPs • Apply restrictions and enhanced security provisions for high-risk MSPs • Impose strict access controls for third line support from equipment manufacturers for sensitive parts of the network	🇫🇮	MNOs are required to ensure that, in a state of emergency, critical systems and their guidance, maintenance and control can be returned to Finland without delay. Regulator also has the power to issue regulations relating to network management
More examples			🇸🇪	The Swedish Post and Telecom Authority (PTS) has placed limits on the types of activity and conditions under which MNOs are able to outsource functions to MSPs, with MSPs subject to enhanced security provisions in sensitive parts of the 5G networks
			🇵🇱	The Office of Electronic Communications (UKE) has placed limits on the types of activity and conditions under which MNOs are able to outsource functions to MSPs, with MSPs subject to restrictions in sensitive parts of the 5G networks and enhanced security provisions
			🇩🇰	The Danish Business Authority (DBA) imposes strict access controls for equipment manufacturers' third-line support, particularly for critically sensitive components and/or sensitive parts of the network, with suppliers considered to be high-risk subject to enhanced security provisions

2.4. List of the strategic measures (5/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
c) Diversification of suppliers				
SM05	Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies	• Establish multi-vendor strategy for each MNO • Avoid major dependency on a single supplier • Avoid dependency on high-risk suppliers (as per SM03)	🇨🇾	The regulatory framework provides guidelines for MNOs to adopt risk-based multi-vendor strategies. This measure will take into account the need to keep additional burdens on MNOs limited to the minimum necessary
		More examples	🇪🇸	The Spanish government has established guidelines to promote supplier diversification among the MNOs, with the aim of reducing their reliance on individual or high-risk suppliers. These guidelines take into account technical constraints and interoperability requirements to ensure a sustainable and robust telecommunications ecosystem
			🇵🇱	The Polish government has guidelines for MNOs to diversify their suppliers and avoid dependency on single or high-risk ones. Guidelines consider technical constraints and interoperability requirements
			🇩🇰	To encourage a diverse and sustainable telecommunications industry, the Danish government has established guidelines that require MNOs to avoid relying on individual or high-risk suppliers. These guidelines take into account technical constraints and interoperability requirements, ensuring that MNOs have access to a range of reliable suppliers that can support their operations

2.4. List of the strategic measures (6/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
c) Diversification of suppliers				
SM06	Strengthening the resilience at national level	• Establish an adequate balance of suppliers at national level for network resilience • Consider variations in geography and population when selecting suppliers • Ensure resilience in case of incidents with operators or suppliers	🇭🇷	Measures to ensure resilience at national level through an adequate balance of suppliers are under consideration to be included in relevant legal acts
		More examples	🇸🇪	The Swedish Post and Telecom Authority (Swedish PTS) established guidelines for MNOs to ensure an adequate balance of suppliers at the national level for resilience in case of incidents with one operator/supplier
			🇮🇹	The Italian government has a legal/regulatory framework requiring MNOs to ensure an adequate balance of suppliers at the national level for resilience in case of incidents with one operator/supplier
			🇩🇰	The Danish government established guidelines for MNOs to ensure an adequate balance of suppliers at the national level for resilience in case of incidents with one operator/supplier

2.4. List of the strategic measures (7/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
d) Sustainability and diversity of 5G supply and value chain				
SM07	Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU	• Enhance Foreign Direct Investment (FDI) monitoring in 5G value chain to detect threats to security or public order • Investigate trade-distorting behavior of producers falling under EU anti-dumping and anti-subsidy rules • Evaluate FDI based on risk profile of buyers/companies for critical infrastructure, public security, access to and control of information and cybersecurity	🇪🇺	In addition to the EU level FDI screening Regulation applied in October 2020, more than 14 EU Member States have their own national screening mechanisms, thus creating a comprehensive framework for screening foreign investments
More examples			🇫🇷	The French government has established a legal/regulatory framework that identifies key assets in the 5G value chain and fosters a diverse and sustainable 5G ecosystem in the EU. The French government has also established guidelines for the monitoring of FDIs across the 5G value chain to better detect foreign investments that may pose a threat to the security or public order of France or other EU member states
			🇧🇪	The Belgian government has established guidelines for the monitoring of FDIs across the 5G value chain to better detect foreign investments that may pose a threat to the security or public order of Belgium or other EU member states. The guidelines also encourage the identification of key assets in the 5G value chain and the fostering of a diverse and sustainable 5G ecosystem in the EU

2.4. List of the strategic measures (8/8)

STRATEGIC MEASURES

Id	Measure	Description	Co.	Illustrative cases
d) Sustainability and diversity of 5G supply and value chain				
SM08	Maintaining and building diversity and EU capacities in future network technologies	• Foster a diverse, sustainable, and secure 5G ecosystem through policy and innovation support • Ensure supplier diversity and knowledge through EU partnerships • Support innovation and overcome failures with EU funding and initiatives	🇫🇮	The Finnish government has established policies to create optimal conditions for European technological firms and foster innovation in key technology areas to promote a diverse, sustainable and secure European 5G ecosystem. Finland has been actively involved in the development of the proposed EU Institutionalized partnership in the field of NGI/6G ("Smart Networks and Services") 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
More examples			🇮🇹	The Italian government has established policies to support the development of EU capacities and avoid dependencies by supporting disruptive and ambitious research & innovation. Italy has been actively involved in the implementation of the various EU funding programs, including Horizon Europe, the Digital Europe Program, and the Connecting Europe Facility (CEF). Italy has also launched initiatives such as 5G Corridors for Connected and Automated Mobility to support the development of diverse, sustainable, and secure 5G ecosystems
			🇪🇸	The Spanish government has established policies to bring together knowledge, expertise, financial resources, and economic actors throughout the Union to overcome potential important market or systemic failures along the value chain. Spain has established an Important Project of Common European Interest (IPCEI) to support the development of key technologies and promote a diverse, sustainable, and secure European 5G ecosystem

2.5. Technical measure - responsible unit

RESPONSIBILITY FOR IMPLEMENTATION

Measures	Relevant actors				
	Member States' Authorities	Mobile Network Operators	European Comission	ENISA	Stakeholders (incl. Suppliers)
TM01 - Ensuring the application of baseline security requirements	✓	✓			
TM02 - Ensuring and evaluating the implementation of security measures in existing 5G standards	✓	✓			✓
TM03 - Ensuring strict access controls	✓	✓			
TM04 - Increasing the security of virtualized 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	✓		✓	✓	✓
TM11 - Reinforcing resilience and continuity plans	✓	✓			✓

2.6. List of the technical measures (1/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
a) Network security - baseline measures				
TM01	Ensuring the application of baseline security requirements	• Implement security best practices and risk assessments • Keep up-to-date security policy and procedures • Ensure adherence to security best practices	🇨🇾	MNOs follow security protocols, but need to reinforce measures with baselines and audits. Cyprus' Digital Security Authority aims to add application-layer security requirements for operators based on guidelines.
More examples			🇩🇪	The government has set security requirements for 5G networks, including baseline requirements for secure network design and architecture. Operators must implement existing security best practices and recommendations, and conduct regular risk assessments
			🇫🇷	The government has established a cybersecurity framework for 5G networks, requiring operators to implement security best practices and maintain up-to-date information on security policy and procedures. Regular security audits and assessments are also required
			🇮🇹	The government has established a national security framework for 5G networks, including baseline requirements for secure network design and architecture. Operators must implement security best practices and maintain up-to-date information on security policy and procedures. Regular security audits and assessments are also required

2.6. List of the technical measures (2/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
a) Network security - baseline measures				
TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards	• Implement 5G technology standards as a minimum security baseline • Ensure adequate implementation of optional security measures in 5G standards • Require MNOs and suppliers to comply with relevant 5G security standards	🇦🇹	In the Telecom Network Security Regulation ("TNSR"), MNOs operating a 5G network will have to comply with essential 3GPP security standards
		More examples	🇫🇷	The French government ensures and evaluates the implementation of security measures in existing 5G standards, such as 3GPP, and requires operators and suppliers to use it as a minimum security baseline for MNOs. The government has also established a national cybersecurity agency, ANSSI, which provides guidance and support to operators and suppliers on the implementation of security measures in 5G networks
b) Network security – 5G specific measures				
TM03	Ensuring strict access controls	• MNOs should enforce strict network access controls and minimize remote access by high-risk third-party suppliers • The principle of least privilege should be applied to various network rights • MNOs should have procedures in place to ensure that these rules are always in effect and evolve with the network	🇮🇪	The Telecoms Security Requirements outline requirements for network design and access control, such as network segmentation, access control, multi-factor authentication (MFA), and separation of duties. Operators must also implement logging and monitoring to detect abnormal access activity
		More examples	🇵🇹	The Portuguese government requires MNOs to implement strict access controls for 5G networks, including network access controls, the principle of least privilege, and the segregation of duties principle. The government has established a dedicated 5G security center to provide guidance and support to operators and suppliers on how to implement strict access controls and other security measures in 5G networks

2.6. List of the technical measures (3/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Network security – 5G specific measures				
TM04	Increasing the security of virtualized network functions	• Follow security best practices for network function virtualization • Consider physical separation for critical or sensitive network functions • Ensure appropriate security measures for all network functions	🇦🇹	In the Telecom Network Security Regulation (TNSR), MNOs operating a 5G network will have to comply with recommendations laid down in the ENISA document 'Security Aspects of Virtualization'
		More examples	🇩🇪	Germany's Federal Network Agency requires MNOs to follow security best practices for network function virtualization. The agency has issued guidelines and recommendations to ensure that MNOs implement adequate technical measures to secure their networks
			🇫🇷	The French government has established a security framework for 5G networks that includes requirements for MNOs to follow security best practices for network function virtualization. The framework includes guidelines for network security, data protection, and incident response

2.6. List of the technical measures (4/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Network security – 5G specific measures				
TM05	Ensuring secure 5G network management, operation and monitoring	• MNOs must operate their NOC (Network Operation Centers) and SOC (Security Operation Centers) on premise, inside the country and/or inside the EU for secure network management • NOC and SOC must implement effective network monitoring of critical components and sensitive parts of 5G networks to detect and avoid threats • MNOs should protect management traffic to prevent unauthorized changes to the communications network or service components	🇮🇹	Baseline requirements for this technical measure are outlined in the Ministry of Economic Development's Decree on "Security and Integrity Measures of Electronic Communication Networks" (2018). MNOs are not allowed to outsource their Network Operations Centers and maintain network management autonomy under Golden Power regulations
		More examples	🇩🇪	German MNOs must run their NOCs and SOCs on premise or inside the EU, monitored by the German Federal Office for Information Security
			🇩🇰	Danish MNOs must establish NOCs and SOCs for effective network monitoring and comply with security audits

2.6. List of the technical measures (5/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Network security – 5G specific measures				
TM06	Reinforcing physical security	• Ensure physical protection of critical components and sensitive parts of 5G networks • Apply a risk-based approach to reinforce physical access controls for MEC and base stations • Limit and monitor access by third-parties, contractors, and employees of suppliers/vendors, integrators	🇦🇹	According to the TNSR, MNOs operating a 5G network will explicitly have to ensure physical security of critical network components and sensible parts with regard to Multi-Access Edge Computing and base stations
More examples			🇩🇪	In Germany, MNOs are required to protect critical components and sensitive parts of the 5G network through physical access controls. For example, MNOs must ensure that only authorized personnel have access to the 5G core network, and that access is monitored and logged
			🇮🇹	In Italy, MNOs are required to implement appropriate physical access controls for critical components and sensitive parts of 5G networks. This includes measures such as secure storage facilities, controlled access to data centers, and the use of encryption to protect sensitive data in transit

2.6. List of the technical measures (6/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
b) Network security – 5G specific measures				
TM07	Reinforcing software integrity, update and patch management	• Deploy adequate tools and processes for software integrity • Identify and keep track of changes and patch status • Perform software updates and apply security patches in 5G networks	🇳🇱	The technical and organizational security requirements, including access control, security patching, incident detection, network segmentation, and third-party software security, will be established in secondary legislation under the Telecommunications Act
		More examples	🇩🇪	Germany requires MNOs to deploy tools for automated and secure software updates and patch management. They also conduct regular security audits and require security certifications[6] from their suppliers

[6] In Germany, suppliers can obtain the necessary certifications by undergoing an assessment process by an independent auditing body. The assessment process includes a review of the supplier's documentation and systems, and a penetration test to verify the security of the 5G equipment

2.6. List of the technical measures (7/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
c) Requirements related to suppliers' processes and equipment				
TM08	Raising the security standards in suppliers' processes through robust procurement conditions	• Demand specific security standards from equipment suppliers during procurement process • Require equipment suppliers to demonstrate quality levels and security maintenance throughout the lifetime of equipment • Ensure that security is built into the product development processes of equipment suppliers	🇮🇪	The TSRs mandate operators to incorporate security requirements into their testing and evaluation process, which includes assessing a supplier's product lifecycle and security management. Operators are also required to include clauses pertaining to product lifecycle and security management in their contractual arrangements with suppliers
More examples			🇫🇷	In 2019, the French government introduced new security requirements for operators and equipment suppliers, including the need to obtain certification from the French cybersecurity agency ANSSI. This certification includes requirements for secure product development, supply chain security, and continuous monitoring and maintenance of equipment
			🇬🇧	In 2020, the UK government announced new rules that would ban the use of Huawei equipment in the country's 5G networks and require operators to remove existing Huawei equipment by 2027. The government also introduced a Telecoms Security Bill, which includes provisions for mandatory security requirements for network equipment suppliers and fines for non-compliance

2.6. List of the technical measures (8/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
c) Requirements related to suppliers' processes and equipment				
TM09	Using EU certification for 5G network components, customer equipment and/or suppliers' processes	• Consider including relevant EU-wide schemes for critical network components and 5G customer equipment in Union Rolling Work Programme • Evaluate if certification or supplier's process can be added to the Union Rolling Work Programme • Certify critical network components used in 5G networks and 5G customer equipment under the EU certification framework	🇪🇺	ENISA, the European Commission supported by working groups (Ad-Hoc Working groups) representing the ecosystem and Member State competent authorities are working together to establish the first certification schemes A first draft of the scheme should be available for public consultation around mid-2023
TM10	Using EU certification for other non 5G-specific ICT products and services	• Consider adding EU-wide certification schemes for non-5G ICT products and services to the Union Rolling Work Programme • Include schemes for the security of cloud services and related technologies • Include schemes for the security of connected devices, including IoT	🇪🇺	

2.6. List of the technical measures (9/9)

TECHNICAL MEASURES

Id	Measure	Description	Co.	Illustrative cases
d) Resilience and continuity				
TM11	Reinforcing resilience and continuity plans	• MNOs should reinforce their resilience and continuity plans • Adequate plans should be in place in case of disaster affecting network operation • MNOs should request similar arrangements from suppliers and only use those who demonstrate sufficient long-term resilience	🇧🇪	Risk assessments, including the security measures in place are reported to the National Regulatory Authority (NRA). In the context of critical infrastructure, which includes 5G, the NRA monitors the regular execution of continuity exercises by operators. The NRA maintains a sectoral telecommunication crisis plan and organizes periodic exercises
		More examples	🇩🇪	The Federal Network Agency requires MNOs to establish business continuity and disaster recovery plans for their networks. These plans must address risks and vulnerabilities, outline processes for mitigating them, and include testing and updating procedures. MNOs are also required to assess and mitigate dependencies on their suppliers and other third-party service providers
			🇬🇧	The UK government has established a Cyber Security Information Sharing Partnership (CiSP), which provides a secure platform for government agencies, businesses, and other organizations to share information about cyber threats and vulnerabilities. MNOs are encouraged to participate in this partnership and share information about their resilience and continuity plans

2.7. How the EU supports Member States

Objectives of the European Union Agency for Cybersecurity

ENISA is the European Union's agency focused on achieving a high level of cybersecurity across Europe. Since its establishment in 2004, and bolstered by the EU Cybersecurity Act, ENISA has contributed to EU cyber policy and enhanced the reliability of ICT products, services, and processes through cybersecurity certification schemes. It collaborates with EU bodies and Member States and prepares Europe for future cyber challenges. ENISA shares knowledge, builds capacity, and raises awareness to work alongside its key stakeholders in strengthening trust in the connected economy, boosting the resilience of the EU's infrastructure, and ensuring digital security for Europe's society and citizens.

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

How the ENISA supports EU member countries in the implementing of the Cybersecurity processes and tools

NFV Security in 5G - Challenges and Best Practices

In this report explores relevant challenges, vulnerabilities and attacks to the Network Function Virtualization (NFV) within the 5G network. NFV changes the network security environment due to resource pools based on cloud computing and open network architecture.

5G Cybersecurity Standards

This report outlines the contribution of standardization to the mitigation of technical risks, and therefore to trust and resilience, in the 5G ecosystem. This report focuses on standardization from a technical and organizational perspective.

ENISA Threat Landscape for 5G Networks Report

The vulnerability and threat assessments found in this document introduce a significant advancement to the previous edition, by providing more comprehensive information about the exposure of assets of the updated 5G architecture.

Fog and Edge Computing in 5G

Fog and edge computing have become key enablers in the 5G ecosystem, creating new opportunities and novel applications, but also multi-modal security challenges, that the telco, cloud and industrial communities address them from different perspectives.

3. EU approach to define High Risk Vendors (SM03)

3.1. Legal bases for HRV assessment procedure

EU legal basis – NIS2 Directive

Art. 7 par. 1: Each Member State shall adopt a **national cybersecurity strategy** that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:

[...]

(b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, **including the policies referred to in paragraph 2**

(c) a **governance framework** clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts

+

Art. 7 par. 2: As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing **cybersecurity in the supply chain for ICT products and ICT services** used by entities for the provision of their services;

+

Criteria for HRV definition

Legal frameworks among Member States vary, the general criteria to assess the vendor were defined in par 2.37. of EU coordinated risk assessment of the cybersecurity of 5G networks

Examples of assessment criteria already established by a few Member States are:

- **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. 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;
- the characteristics of the supplier's corporate ownership;
- 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 prioritization is given to security practices.**

3.2. Example case studies of the approach of Member States[7] to High-Risk Vendors (1/3)

High-Risk Vendor definition

Category	Description	Co.	Illustrative cases
‘Deny list’ approach (ex-ante)	Designating certain suppliers as high risk or untrusted and on this basis, applying restrictions or bans for operators to source certain equipment or services from them; restrictions under consideration may take the form of exclusions and/or caps on the share of the supplier(s) in the networks.	🇸🇪	In 2020, Swedish telecom regulator PTS unexpectedly banned a particular technology provider from supplying 5G equipment to Swedish mobile firms citing security concerns raised by Sweden's security service, a decision the company challenged in the court, which upheld the decision of PTS
		🇬🇧	In 2020, the decision was taken by the National Security Council, in response to US sanctions imposed on one technology provider to ban and remove in from the infrastructure of 5G networks
		🇵🇱	Proposed solution would allow the minister responsible for informatization to declare a provider as a HRV based on the security risk assessment performed by the dedicated advisory body
		🇸🇮	There are attempts to introduce an act which would allow the dedicated advisory body to declare a provider as a HRV

[7] The United Kingdom until the 31st of January 2020

3.2. Example case studies of the approach of Member States to High-Risk Vendors (2/3)

High-Risk Vendor definition

Category	Description	Co.	Illustrative cases
Pre-authorization or notification/veto approach (ex-ante)	Assessing operators' plans and imposing restrictions or exclusions on a case-by-case basis, taking into consideration a variety of aspects, including the characteristics of individual suppliers as well as specific deployment modalities	🇫🇷	Recently established process introduces a new prior authorization regime for the use of 5G network devices by operators
		🇪🇪	Introduced legal acts established a procedure of cybersecurity certification in order to allow the Consumer Protection and Technical Regulatory Authority to review security risks among technology providers
		🇷🇴	The authorization procedure for manufacturers involves an assessment conducted by Romanian authorities to confirm that the applicant is not subject to control by a foreign government, has a transparent ownership structure, and is subject to a legal regime that enforces transparent corporate practices

3.2. Example case studies of the approach of Member States to High-Risk Vendors (3/3)

High-Risk Vendor definition

Category	Description	Co.	Illustrative cases
Monitoring (ex-post)	Member State left the decision regarding the choice of providers to operators, with indication of potential steps in case of circumstances harming the security of the Member State.	🇦🇹	In Austria, the responsibility of selecting 5G providers lies with the operators. The government has established a non-political expert advisory board to evaluate and oversee the risks associated with the 5G suppliers chosen by these operators.
		🇱🇺	Prime Minister of the Grand Duchy of Luxembourg stated that the operators' criteria covered both financial and technological aspects, adding that a "geostrategic sensitivity" should be taken into account when seeking suppliers
		🇮🇪	Minister for the Environment, Climate and Communications may assess at any time, and on an ongoing basis, the likelihood of a vendor being subjected to interference by a third country