National 5G Cybersecurity Risk Assessment of the Republic of Slovenia

The National 5G Cybersecurity Risk Assessment of the Republic of Slovenia was prepared based on the contributions of four telecom operators (Telekom Slovenije, T-2, Telemach, A1) and national authorities responsible for national security (Ministry of the Interior, the Police, Ministry of Defence, Slovene Intelligence and Security Agency, Government Office for the Protection of Classified Information) jointly coordinated by the Agency for Communication Networks and Services and the Ministry of Public Administration.

Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings

1 Introduction

The Commission Recommendation (EU) 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks (hereafter 'the Recommendation') sets out a number of concrete actions. In particular, it requests each Member State to carry out a **national risk assessment** of the 5G network infrastructure by 30 June 2019 and to transmit the results to the Commission and to ENISA **by 15 July 2019.**

On the basis of the national risk assessment and taking into account ongoing coordinated action at EU level, the Recommendation provides that **each Member State should review and update applicable security measures**, including 'reinforced obligations on suppliers and operators to ensure the security of sensitive parts of the networks', as well as other obligations, where appropriate.

In parallel, the national risk assessments should form the basis for a **coordinated Union risk assessment**, to be produced **by 1 October 2019**. The coordinated Union risk assessment should be made up of a threat landscape mapping to be conducted by ENISA and a joint review of the Union-wide exposure to risks to be conducted by Member States, with the support from the Commission and together with ENISA.

At the first meeting of the dedicated NIS Cooperation group on 11 April, Member States authorities discussed national risk assessments processes and identified a number of possible elements for a common approach. After the meeting, a first outline was shared with Member States for comments in order to prepare these draft guidelines and structured template, on which Member States were also asked to provide comments.

2 Aim and Scope

This document sets out a set of guidelines on **common elements for national risk assessments** and a **structured template for reporting on the main findings**.

Its purpose is two-fold: (i) promoting consistent approaches in national risk assessments and (ii) facilitating the exchange of relevant and comparable information among Member States to inform their national processes and facilitating the preparation of the EU coordinated risk assessment.

This document builds on the definitions and provisions of the Recommendation and also reflects the discussion and information shared by Member States on their national approaches at the dedicated meeting of the NIS Cooperation Group that took place on 11 April, as well as further input provided by ENISA and by several Member States after this meeting.

Data exchange process

By 15 July, Member States are invited to send:

1. Responses to the questions included in this structured template, to be shared with other Member States and with the Commission and ENISA.
2. The full results of the national risk assessment (excluding classified information) to the Commission and ENISA.

Member State should submit their reports and responses to a dedicated CIRCA address.

3 Common elements for 5G cybersecurity risk assessments and structured template for reporting on findings

As set out in the Recommendation, Member States should carry out a risk assessment of the 5G network infrastructure by 30 June 2019 and transmit the results to the Commission and ENISA by 15 July 2019.

These guidelines do not address risk assessment methodologies in detail. Authorities could use several standard methodologies for performing their national risk assessments of 5G networks (eg. ISO/IEC: 27005).

These guidelines and structured template aim to facilitate a consistent approach and a common understanding of the risks, including for preparing the EU coordinated risk assessment. To this end and while applying the risk assessment methodologies of their choice, Member States are invited to consider the elements listed below in their national risk assessments of 5G cybersecurity and to provide a summary of the findings using the structured template set out therein.

Responses to the questions included in the template should be based on the results of the national 5G cybersecurity risk assessments.

The responses provided should reflect the assessment of the risks at national level from the perspective of the governments (ie. legislators/regulators), supported by other stakeholders' views (including network operators or suppliers) where necessary.

The guidelines and template set out below reflect an approach based on the identification of assets, threats, and vulnerabilities to help identify potential ways, in which threat actors could exploit a certain vulnerability of an asset to impact on the government's objectives. On this basis, end-to-end risk scenarios linking these different elements will be key to identify the main risks to the cybersecurity of 5G networks.

3.1 Definition. The Recommendation provides that 5G networks means 'a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy network elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network'.

3.2 Cybersecurity threats. National risk assessments should identify the top level threats and their relevance in the case of 5G networks. They should include the following high-level categories of cybersecurity threats and threat actors as well as an assessment of the relevance of the threat based on the capabilities and intent of the threat actors:

3.2.1. Main threat actors

- *non-adversary/accidental threat actor, such as an unintended impact or a side effect from an operation not targeting the operation of a mobile communication network*
- *an individual hacker*
- *a hacktivist group*
- *an organized crime group*
- *an insider*
- *a nation state or nation state-backed actor*

3.2.2. Main threats

- *Compromised confidentiality (incl. espionage)*
- *Compromised availability*
- *Compromised integrity of a service*

SUMMARY OF FINDINGS ON MAIN THREATS

Question 1: Please fill the table below, associating the main threats and threat actors, and provide a rating of 1 to 5 according to their relevance (assessed by taking into account capabilities and intent) of the various combinations.

Relevance rating: 1= Very high; 2= High; 3= Medium; 4= Low; 5= Very low

Threat actors / Threats	Non-adversary /accidental	Individual hacker	Hacktivist group	Organized crime group	Insider within a telecom operator or subcontractor	Nation state or nation state-backed actor
Compromised confidentiality	4	3	3	2	3	2
Compromised availability	3	4	3	3	3	2
Compromised integrity	4	4	3	2	3	2

Comments/additional information:

It is a non-quantified assessment, prediction and of course does not apply to the 5G itself as such. In general, we believe that a possible transition to the 5G does not mean a significant change in the approach and the security aspect - the latter is very important and a major challenge also in the current 2G / 3G / 4G networks from a technological, processes and human resources points of view. Naturally, with 5G there is a significantly greater complexity (technologically), and if the 5G is used as main communication platform for verticals, such as health, energy, transport and smart factories - the risks would, of course, increase exponentially.

The most relevant threat actor in this assessment is nation state or nation state-backed actor with both high capabilities and intent for compromising 5G networks. Not far behind is organized crime group which too can poses a significant level of capabilities and intent. Telecom operators who were involved in the preparation of the risk assessment also ranked high insider within a telecom operator or subcontractor but considering other contributors to the assessment, that threat actor ended as medium relevant.

A case of large 5G operator's presence in different countries should also be considered. For example, such big operator can have some of its core equipment installed in one country and carries out services (and data) in other countries. An attack by any of the threat actors on operator's core equipment in a domestic country would also affect services in other countries.

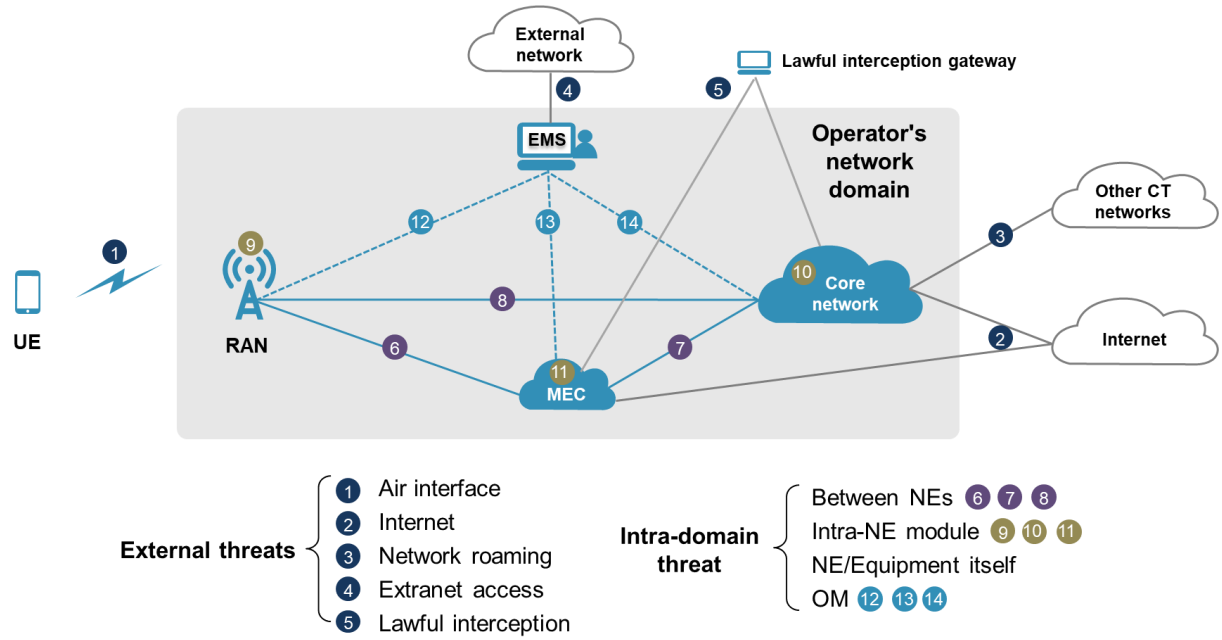
Question 2: Please describe the main threat scenarios related to 5G, which were considered in your national risk assessment?

Main threat scenarios	Description
Compromised availability of the critical infrastructure (e.g. electricity supply, traffic systems) and breaches in state IT systems	Security breach in availability of electricity supply caused by any of the threat actors would compromise availability of mobile infrastructure and cause serious disruption or interruption of services (including emergency services). Such breach can consequently also cause serious disruption or interruption of services in all other sectors of critical infrastructure. Interrupted availability of road traffic management data and the network would cause confusion in road traffic. Owner or important affiliate of the network under threat is strongly positioned in potential adversary, as well as key vendor, part of network and IT including IoT platform is hosted in potential adversary and other countries. Part of operations is outsourced to the vendor. Breaches within state IT systems for espionage caused by foreign intelligence services would have profound impact on national security.
Compromised availability of vendors' technical support and threats related to human resources	Due to high complexity of mobile infrastructure, technical support in terms of new software updates and releases is critical to maintain integrity, confidentiality and availability of it. High level of maintenance support is crucial to support operator's own maintenance activities. Set of risks related to human resources and human factors in both vendor and operator include lack of skills, lack of awareness, negligence, unauthorised changes, loss of key personnel etc.
Network equipment, deployment and operation security	Security challenges brought by new services, architectures, and technologies to 5G networks need to be considered. For example, in terms of new services, consideration must be given to access authentication for third-party slicing service providers. 3GPP is considering security challenges and solutions to the new 5G architectures, such as network slicing and Service Based Architecture (SBA). With wide application of cloud architecture in 5G, secure use of computing assets must also be considered, as well as developing new technologies such as quantum computing and its impact on traditional cryptographic algorithms.

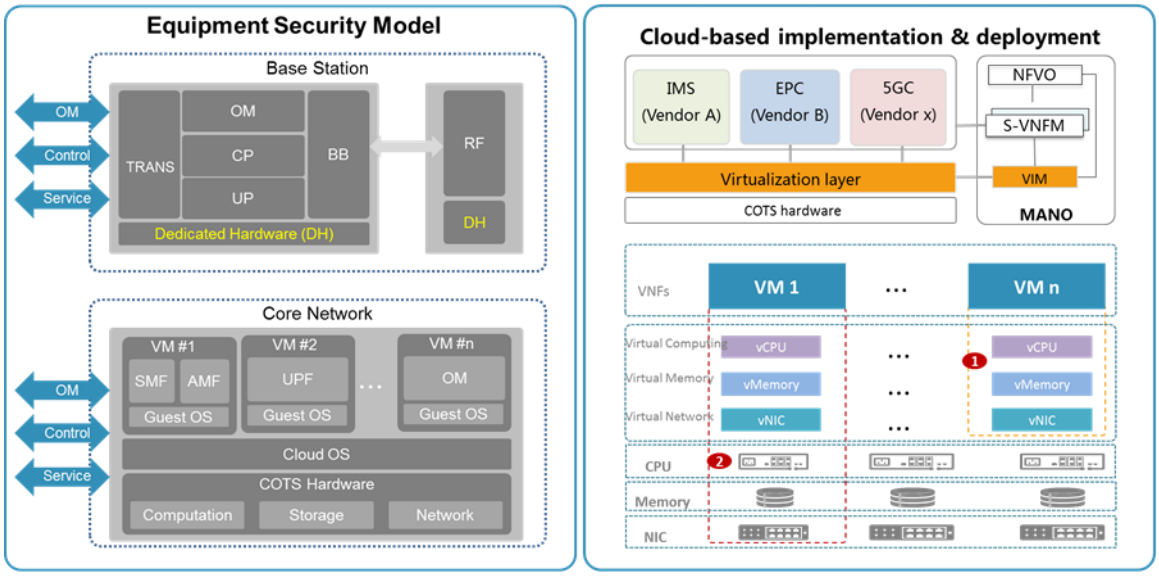
Challenges related to the use of network equipment, its deployment and operation security

MEC and other 5G application servers: MEC (Mobile Edge Computing), as a core network entity deployed after UPF, may be deployed in a distributed machine room. Compared with central machine room, it is less physically protected, e.g. less administration, less CCTV etc. So MEC may face more threat as a hacker may physically interfere with the MEC equipment. In addition, MEC integrate more 3rd party APPs, which may also bring potential threat, as the 3rd party APPs may be the security weakest link of the whole system.

The figure below illustrates an overview of threat scenarios from network point of view. The threat scenarios include two types: outside operator's domain and inside operator's domain.



If we further investigate the equipment, e.g. implementation level, we could find below a general view on what might be the key assets to protect and their main threat scenarios.



It would be useful to note that the cloud (or virtualized) implementation which is based on COTS hardware is just one of the implementation options. The other option is to rely on specific designed and thus highly efficient hardware (FPGA, ASIC, etc).

The COTS hardware-based option is an option that might introduce more complexity to the system's security design since it brings more modules (some based on open source software which brings more uncertainty from a maintenance point of view), and thus more stakeholders which makes it more difficult to provide for an end-to-end security at equipment level.

Type	Main threat scenarios	Description
Outside operator's domain	Air interface security threats	The threat exists between the network and a User equipment. This is a standardized interface.
	Internet access security threats	The threat exists between a gateway function of an operator and an Internet service (or a packet data network, PDN).
	Roaming security threats	The threat exists in the roaming interface related to two different operators which are visited operator and home operator.
	Security threats of external access to EMS	The threat exists between the management server inside an operator network domain and management client outside the operator network domain.
	Lawful interception security threats	The threat is related to unauthorised access to lawful interception interfaces between core network functions and lawful interception function which is outside the operator's network.
Inside operator's domain	Between NEs, including SBA threats within 5GC, threats among 5GC/MEC/gNodeB	5G Core introduces new Service Based Architecture, which may lead to a new threat. • gNodeB and 5GC/MEC deployed in the different security domain. Threats are related to the signal and user data transmission between gNodeB and 5GC/MEC • Threats to the clock interface: clock server spoofing, clock information tampering, GPS clock interference • Threats to the transmission interface: communication entity spoofing, Information eavesdropping, Information tampering, DoS attacks
	Intra-NE module, including threats within MEC, threats to cloud security, threats to slicing security	Mobile edge computing is not defined in 3GPP's first 5G release (e.g. Release 15) but it is foreseen that it might be widely used in 5G. The distributed locations hosting MEC equipment are not as well physically protected as central server rooms which normally hosts sensitive core network devices. In addition, MEC may integrate third-party APPs. Both may lead to potential threats. NFV is introduced already in 4G vEPC, while 5G core will be fully cloudified. As a result, threats to cloud computing security are very important issue of 5G. 5G introduces E2E slicing, which will share the same infrastructure resources, but provide different QoS, security, quality services based on different slices. The new technique may bring new threats.

Type	Main threat scenarios	Description
	NE/equipment itself, including threats to software and hardware security, threats to data security	Devices hardware has some physical interfaces, the threat to hardware comes from unauthorised access to these physical interfaces at local site. Threats to hardware: illegal intrusion, unauthorized access to or control of gNodeBs, theft of some hardware, physical damage. The threats to software involve unauthorized operations, malicious software implantation and tampering before installation.
	O&M security threat	Threats on OAM interface: unauthorized access, privilege escalation or abuse, brute force user account/password cracking, maintenance data tampering and leakage, system fraud, system time tampering, web security threats.

3.3 Assets: what do we want to protect? As set out in the Recommendation, national risk assessment of 5G should include 'identifying the most sensitive elements where security breaches would have a significant negative impact. For this purpose, national risk assessments should consider the following categories of assets and provide an assessment of their level of sensitivity:

- *Network components and/or functions*
- *Specific areas, based in particular on the number of potential affected users*
- *User groups (examples: key governmental entities, law enforcement or military assets, critical infrastructure operators/ operators of essential services, etc.)*

To identify areas or user groups, where security breaches would have a significant impact, the following categories of potential impacts could be considered:

- *National fundamental interests, sovereignty and democracy*
- *Public and interior security, including emergency services and preparedness*
- *Population and environment*
- *Economy/GDP*
- *Personal data protection*
- *Intellectual property protection*

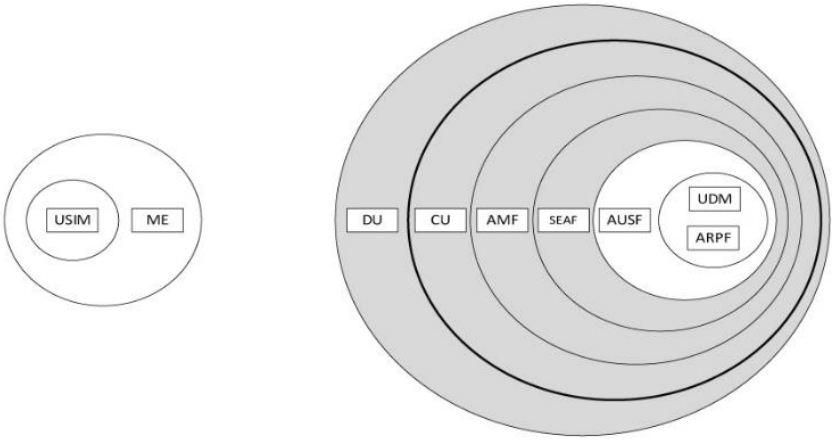
SUMMARY OF FINDINGS ON MAIN ASSETS

Question 3: Based on your national 5G risk assessment, have you identified specific sensitive network components or functions?

Yes/No

If possible, please indicate which ones:

As a reference, a trusted model of 5G network is cited below from 3GPP website. Trust within the network is considered as decreasing the further one moves from the core, which means that UDM/ARPF requires the highest trust level (e.g. critical) while gNB (DU/CU in the figure) requires the lowest trust level (e.g. sensitive or not sensitive).



Comments/additional information:

From the risk analysis point of view, the sensitivity of the gNB is limited as compared to the core network functions – if a single gNB is compromised, it will impact only users in a given area, not the security of the whole network or all users. Therefore, we consider gNB as non-sensitive by comparison.

Although both UE and service/application are not listed as a network function, it must be noted that they are also sensitive from a security point of view. For eMBB services, UE is exposed to many traditional security threats, malware, etc. which can compromise user privacy even when no network infrastructure is compromised.

One of the big trends in 5G is that many verticals will start to use 5G technologies. From the terminal side, such type of terminal may introduce new types of attacks to the network (e.g. Mirai cyber-attack in 2016 by hijacking IoT devices).

It should be noted, that the ultimate accountability for ensuring appropriate level of security rests with the application provider. The application provider should decide whether to rely on lower-layer security features or use end-to-end application layer security. For example, for bank services used over mobile network, application layer security is used by bank to provide end-to-end security. Another example is that a vehicle control application should ensure safety despite lack of network coverage.

Question 4: If possible, please indicate the relative degree of sensitivity of the various categories of networks elements and functions included in the table below. For each category, if available please provide a more detailed categorisation of specific elements or functions.

	Low	Moderate	High	Critical
Access network functions				
Radio heads with antennas			**x**	
Baseband units			**x**	
Core network functions				
HLR / HSS / UDM				**x**
Packet core				**x**
Transport & transmission functions				
Fibre optic infrastructure			**x**	
Transport equipment			**x**	
IP/MPLS network			**x**	
Internetwork exchanges				
Internetworking links				**x**
Management systems & Supporting Service				
Network management			**x**	
Service management			**x**	
Rating system				**x**
Billing system				**x**
Service systems				
IMS				**x**
SIM cards				**x**

Comments/additional information:

As 5G becomes enabler of critical infrastructure, what will really determine the security of a network is the security of products, deployments and configurations of networks; as well as operational procedures put on top of the standardized features. From the security point of view, the whole 5G network is following a layering & domain-separated model which is defined by ISO 19249. According to this model, all the stakeholders of 5G network should take their own responsibility of securing the network. The 5G ecosystem includes application/service providers (application layer), user device (IoT/smartphone) vendor (user domain), network vendor and operator (network domain).

Then for the network layer, it is critical for the 5G network layered security solutions to follow mature industry standards, e.g. in the 5G area, 3GPP has defined clear security requirements and mechanisms to mitigate the identified security risk or threats. In addition, 3GPP may also use/refer other mature industry security tools defined by other standard bodies (e.g. IETF).

For the security certification or assurance, GSMA has defined a set of standards jointly with 3GPP on it, e.g. NESAS & SCAS. It's strongly recommended that these standards will be followed by different regions/countries which have such requirements.

Question 5: Have you identified areas where the number of potential affected users would have a significant negative impact?

Yes/No

Generally, all sectors of critical infrastructure, especially main undertakings which provides energy, transport, health and information and communication services.

If so, please indicate which thresholds were used to select these areas.

The thresholds for selecting capacities in different sectors of critical infrastructure:
Energy sector

- A capacity whose serious disruption or interruption in its operation may cause the breakdown of the electricity system of the Republic of Slovenia to the extent when the required time for its restoration throughout the territory of the Republic of Slovenia is one week.
- A capacity whose serious disruption or interruption in its operation may lead to an interruption in the supply of electricity for three days in an area of more than 100.000 inhabitants.
- A capacity whose serious disruption or interruption in its operation may lead to the interruption of the supply of petroleum products for more than a week in an area with more than 100.000 inhabitants.
- A capacity whose serious disruption or interruption in its operation may cause the supply of natural gas to be disrupted for more than a week in an area with more than 100.000 inhabitants.

Transport sector

- A capacity whose serious disruption or interruption in its operation may prevent the operation of the railway undertaking on a key direction for at least one week.
- A capacity whose serious disruption or interruption in its operation may prevent port activity in the Koper/Capodistria cargo port (the only Slovenian cargo port) facility for at least a week.
- Any capacity serious disruption or interruption in its operation may prevent air traffic from being carried out in the airspace of the Republic of Slovenia by more than 12 hours.

Health sector

- A capacity whose serious disruption or interruption in its operation may prevent the provision of emergency health services and medical care for more than a week in an area of more than 100.000 inhabitants, except for a less accessible and less sparsely populated geographical area with a population of more than 50.000 inhabitants.

ICT sector

- A capacity whose serious disruption or interruption in its operation may cause four hours of failure of electronic communications networks and services to support the performance of one of the critical infrastructure sectors or the national security system, six hours of failure of electronic public sector services or 24 hours of non-functioning of electronic communications networks and services in an area with more than 50.000 inhabitants.

Comments/additional information:

Due to the development of very high-speed broadband networks and new public sector services (including those provided in the cloud), there will be even more access to various data from the mobile networks. Due to the increased complexity of networks, the interconnection of different networks and the increased number of end-user and M2M devices in the new networks, existing security methods will no longer be so effective. It will be necessary to introduce new methods for managing identities, user approvals, data management, and providing anonymity and confidentiality (the mobile network is already being used for remote access to business services, databases, etc.). The risk will also be increased due to the assumption that different network providers can have different security standards, which will be particularly big problem with roaming. Considering cloud services, it should also be noted that mobile clouds are usually less protected and more vulnerable than conventional ones. With the anticipated increase in number of end-user devices, special attention should be paid to devices-network communication, especially if these devices would be used for providing essential services. In the IT sector there will be increased risk of loss or theft of data in addition to the problem of denial of services.

Question 6: Have you identified specific sensitive user groups?

Yes/No

Governmental bodies, armed forces, intelligence services, the Police/law enforcement agencies, emergency services, critical infrastructure operators/essential services providers (e.g. energy, health, transport…).

If so, please indicate which criteria were used to select these user groups.

- Responsibility for assuring fundamental national interests, sovereignty and democracy (governmental bodies, armed forces, intelligence services);
- Responsibility for assuring public and interior security (the Police/law enforcement agencies, emergency services);
- Responsibility for providing essential services (critical infrastructure operators/essential services providers).

Comments/additional information:

Increased use of mobile networks for access to services will result in increased risks for the protection of end users' personal data. Mobile phones are one of the most vulnerable devices and their even wider use for various public sector services will increase the risk of loss or theft of end-user's personal data (e.g. through packet sniffing, (D)DoS on end-user devices, address impersonation, session hijacking,...). Even encrypted communication is not secure if an attack occurs on an unprotected device itself.

3.4 Vulnerabilities. According to the Recommendation, vulnerabilities in 5G networks can originate from various factors, including technical factors and other factors.

While national risk assessments should review any relevant vulnerabilities, they should include the following set of key vulnerabilities.

3.4.1 Vulnerabilities related to technical factors

- *Software-related vulnerabilities*
- *Hardware-related vulnerabilities*
- *Process- related vulnerabilities (including access controls and network architecture), configuration related vulnerabilities)*

3.4.2 Vulnerabilities related to other factors

- *Policy related or organisational vulnerabilities (including people, and outsourcing)*
- *Supplier-related vulnerabilities, including when arising from the legal and policy framework to which 5G equipment suppliers may be subject in third countries*[1]
- *Dependency from one/a limited number of suppliers*
- *Other supply chain vulnerabilities*

[1] As far as risks related to other factors are concerned, the Recommendation states that they 'may include regulatory or other requirements imposed on information and communications technologies equipment suppliers. An assessment of the significance of such factors would need to take into account, inter alia, the overall risk of influence by a third country, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection between the Union and the third country concerned, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection. '

SUMMARY OF FINDINGS ON MAIN VULNERABILITIES

Question 7: Please indicate the most relevant and critical vulnerabilities in each category and indicate whether they are specific to 5G as a whole network or increase with 5G.

a) Vulnerabilities related to technical factors

Types	Main vulnerabilities	Specific to 5G? or increase with 5G (Specific/Increase)	Specific to certain network elements? If so, please indicate which ones?
Software-related vulnerabilities	SW bugs (in products and/or updates)	Increase	
	Harmful SW and backdoors	Increase	Core elements
	Insufficient testing due to fast development	Increase	
Hardware-related vulnerabilities (including IoT)	HW faults	Increase	
	Non-compatible equipment	Increase	
	Insufficient capacity	Increase	
	Lack of redundancy	Increase	
Process-related vulnerabilities	Lack of internal controls in planning and operations	Increase	
	Lack of ability to control outsourcing, subcontractors	Increase	
	Lack of competence regarding verticals specific security requirements	Specific	
	False configuration	Increase	

b) Vulnerabilities related to other factors (non-technical)

Types	Main vulnerabilities	Specific to 5G? or increase with 5G (Specific/Increase)	Specific to certain network elements? If so, please indicate which ones?
Policy and other organisational vulnerabilities	Lack of skilled personnel	Increase	
	Lack of network planning and operations competence in verticals (if they are reluctant to utilize NWaaS capabilities of public 4G/5G networks)	Specific	

	Affiliates heavily dependent or managed by foreign based operator/owner	Increase	
	Bad security specifications and/or lack of security measures due to saving	Increase	
	Lack of knowledge and experience	Increase	
Supplier-related vulnerabilities	Limited local aftersales, technical and maintenance support	Increase	
	Supplier staff, especially when positioned in a country having strong economic or political interest against network users or owners	Increase	
Dependency from one/a limited number of suppliers	Vendor lock-in	Increase	All network – almost impossible to have multi-vendor 5G network in a single country
	High bargaining power of suppliers	Increase	
	Higher price of equipment and services	Increase	
	Long delivery times	Increase	
	Potential lower quality and lacking behind in R&D	Increase	
Other supply chain vulnerabilities	Lack of legal regulation for supply chain	Increase	
	Government restrictions on certain vendors	Increase	
	Legal obligation of cooperation with foreign intelligence services (e.g. China's National Intelligence Law)	Increase	

3.5 End-to-end risk scenarios

In order to link the different parameters described in this document and based on the replies provided in the sections above (threat/threat actors, assets and vulnerabilities), Member States are invited to identify main risk scenarios involving specific threat actors targeting specific sensitive assets and using a specific vulnerability.

Question 8: Please describe the main risks as end-to end scenarios, describing ways how threats could exploit a certain vulnerability of a specific asset, which were considered in your national risk assessment?

Risk scenarios	Description
1.	A cyber-attack on IoT devices in the electricity distribution system through a 5G network by a nation state-backed actor can cause blackouts in large geographic area. That would severely impact various verticals of critical infrastructure as well as interrupt the 5G based services.
2.	A breach of state IT systems by a nation state-backed actor due to combination of backdoor caused by a malware in SW update and equipment misconfiguration. Such clandestine operation used for an espionage and infiltration can severely impact national security with a long run consequence.
3.	The telecom operator procures majority of its communication equipment from a single vendor (vendor lock-in). Due to various reasons (security, political, economic) the vendor's integrity becomes questionable. The operator is faced with possible security risks and even economic/political sanctions but also cheaper and faster network deployment on the one hand and costly equipment substitution and system integration with other vendors' equipment but also avoidance of vendor lock-in with consequences for security and operations in a long run on the other hand.

3.6 Risk mitigating measures. National risk assessment should include an assessment of risk mitigating measures, which are in place or planned and could serve to mitigate the identified risks scenarios, and an assessment of their effectiveness.

This should include the identification of actors, who will need to implement and/or enforce the risk mitigating measures:

- *The network supplier*
- *The outsourced partner that handles field operations or the company operating the network equipment assembly*
- *The delivery chain operator*
- *The telecom operators*
- *The end user (private individual or wholesale user of the 5G services, eg. energy company, hospital, a port or an airport, autonomous driving roadside infrastructure operator)*
- *Targeted Critical Infrastructure operators and Operators of Essential Services.*
- *Key governmental entities/public authorities*

SUMMARY OF FINDINGS ON EXISTING OR PLANNED MEASURES

Question 9: For each of the main risk scenarios identified in the table in question 8, please indicate if mitigating measures are already in place or planned, and if so, which ones, and whether they effectively reduce the likelihood of a vulnerability being exploited.

Risk scenarios	Existing or planned mitigating measures (Yes/No)	Description	Relevant actor (e.g. telecom operator, supplier, etc.)	Effectiveness (Low/Medium /High)
1.	Yes	Denying data services due to DDoS on Internet (should be prevented by application layer)	Telecom operators, equipment supplier	N/A
	Yes (existing)	Unauthorized access to equipment via a physical interface (good physical protection of equipment with access control and status sensors should be implemented, disabling not used physical ports, e.g. serial port, USB port and local ethernet port)	Critical infrastructure operators and operators of essential services	HIGH
	Yes (existing)	Unauthorized remote access (strict access control policy should be implemented)	Critical infrastructure operators and operators of essential services	HIGH
2.	Yes	Spoofing network applications (should be prevented by application layer)	Public authorities, outsourced partner	N/A
	Yes (existing)	Leakage or tampering of user data during transmission (SEPP encrypt and protect the data integrity through TLS protocol)	Telecom operators, network supplier	HIGH
	Yes (existing)	Unauthorized software replacement or malicious software implantation (strict access control policy should be implemented)	Outsourced partner, public authorities	HIGH
	Yes (existing)	Locally stored confidential information is stolen or tampered with, such as keys, and user context information (strict access control, encrypted storage, storage backup, O&M logs and audit should be implemented)	Outsourced partner, public authorities, end user	HIGH
3.	Yes (planned)	Procurement of equipment and services (end-user's (e.g. the state) requirements must be known in advance, supply chain regulation should be adopted and implemented)	Public authorities, end user	HIGH

	Yes (existing)	Planning and deployment (security by default - standards must be followed in planning and deployment phase, interoperability must be guaranteed)	Network supplier, telecom operators, outsourced partner, delivery chain operator	HIGH

Comments/additional information:

Communication operators are undertaking a series of measures to manage the risk in existing 2G/3G/4G network planning and operations, related but not limited to:

- strict procurement process, considering ENISA Security guidelines for ICT procurement,
- benchmarking and rating of vendors,
- strict testing and verification procedure for all technology deployed,
- risk assessment and internal controls related to network planning and operations, ISO 22301 and 27001 compliance,
- cyber security operations centre built beside change management control centre and strongly integrated on e2e service operating centre,
- investments in people and knowledge.

To further strengthen the assurance of security of 5G networks, we suggest taking the following measures:

- Certification schemes in the context of the EU cybersecurity act for critical component to be developed in a joint effort between the industry and the relevant authorities as defined in the Cybersecurity Act (Commission, ENISA, member State representatives, Academia and Industry);
- Security improvements as proposed by GSMA/NESAS for vendor development process accreditation;
- 3GPP SECAM assurance requirements of security functions and product level testing. NESAS and SECAM will provide information to operators and regulators regarding vendors' security by design procedures and the necessary level of appropriateness of vendors' procedures in the development phase such as:
    - Secure Coding Practices,
    - Vulnerability Management.

Certification of equipment at European level by independent verifying entity

Network equipment security certification and assurance is a key tool to evaluate whether such equipment has been designed and implemented so that all the expected security function requirements have been fulfilled. This should be done by independent 3rd party, e.g. professional evaluation/testing laboratories.

The security certification and assurance should follow unified standards to make sure its operation will be cost effective and sustainable for the ecosystem. Now 3GPP and GSMA has defined SCAS (Security Assurance Specification) and NESAS (Network Equipment Security Assurance Scheme) standards set which could be applied for both 4G and 5G.

Now NESAS standards have been completed in GSMA and a pilot test has been done as well. It's expected that NESAS is going to be published this year.

SCAS is defined by 3GPP for each network function (e.g. gNB) of the system. It has defined a set of security function requirement for the targeted network function, which should be fulfilled in the evaluation test. How to do the evaluation test will require a standardized way to do it, which is what NESAS provides.

For NESAS, first clear requirement has been defined on the accreditation process. Then clear audit requirements were defined for the product development procedures and life-cycle management including product planning, development, testing, and maintenance. Such requirement would ensure that the vendor will keep security management embedded in its whole product implementation procedures.

Following common practice of the relevant industries

CVD mechanisms. Now both 3GPP and GSMA is implementing a CVD mechanism so that new vulnerabilities of the network will be identified and resolved timely by the community. It's also very important for the security community of both organizations to clarify potential security 'threat' which might end up as not a real threat after technical analysis.

Cyber security incident response mechanisms: it's also very important for the vendors or operators to timely identify security threats and handled/resolved them in a timely and systematic way.

Any normative or regulation related to 5G security should comply with the following requirements:

Harmonization at European level

EU Member States will start their own internal necessary process with the goal of defining a common EU approach on the issue of cybersecurity of 5G networks. An interface between all the members of the EU to participate cooperatively is highly suggested.

Support of security standardized approaches (GSMA/3GPP)

The underlay infrastructure of 5G networks must comply with security requirements defined in security standards to avoid a disruption in our entire societal processes.

Coordination with additional security initiatives (GDPR, NIS)

Communications networks and services should be built using international and open standards and cybersecurity best practices with the intention to decrease the security risks as much as possible.

Equipment certification

Because a reasonable quantity of security risks in 5G networks are coming from an increasingly cross-border global supply chain which provides ICT equipment, all equipment must be certificated by independent entity at European level. Additionally, risk assessments of supplier's products should be considered, including not only applicable legal environment but also other aspects of supplier's ecosystem to ensure the highest possible level of cybersecurity.

Efficiency in costs

Achieving an adequate level of security not always require heavy costs. Increased costs should be admitted only if security requires it. The financial side of 5G communication networks should meet principles of fairness, be commercially reasonable, and executed openly and transparently.

Minimal impact in Time-To-Market

Guaranteeing a security level is the main aspect of 5G security to maximizes the risks mitigation previously identified. Nevertheless, supply chain and third-party providers should not be affected by.

A more precise list of vulnerabilities related to technical factors (in connection to Question 7 above)

Types	Main vulnerabilities	Specific to 5G? (Yes/No)
Air interface vulnerabilities	Theft/tampering of user data and information	No
	Deny user access due to DDoS	No
	Illegal access to the network by unauthorized terminals	No
	False base station	No
	Trigger terminal fall back to 2G	No
Internet security vulnerabilities	Leakage or tampering of user data during transmission	No
	Spoofing network applications	No
	Denying data services due to DDoS on Internet	No
	Unauthorized access to exposure APIs	Yes
Roaming security vulnerabilities	Leakage or tampering of user data during transmission	No
	Forgery transfer operator and service rejection	No
	Legacy signalling protocols (SS7, diameter) manipulation	No
Lawful interception security vulnerabilities	Illegal interception gateway access	No
	Leakage of the intercepted target ID	No
	Interception data leakage due to attacks from interception port	No
Security vulnerabilities between 5GC/MEC and gNodeB	Data eavesdropping	No
	Data tampering	No
	Unauthorized access	No
Software and hardware security vulnerabilities	Unauthorized access to equipment via a physical interface	No
	Unauthorized operations on NEs	No
	Unauthorized software replacement or malicious software implantation	No
Data vulnerabilities	Locally stored confidential information is stolen or tampered with, such as keys, and user context information.	No
	User privacy information is stolen or tampered with, including subscription data and CDRs.	No
	Unauthorized access to user plane data from other planes.	No
O&M security vulnerabilities	Unauthorized access	No
	Password cracking and leakage	No
	Malicious operations by authorized users	No
	Log deletion/tampering	No
	Sensitive O&M data tampering/leakage	No
	Malware implantation	No
	Web attack (SQL injection)	No
SBA vulnerabilities	DoS deny NRF to register and discover	Yes
	Attacker imitate NFs to access unauthorized data	Yes
	Eavesdrop and tamper data among NFs	Yes

	Attack based on the existed HTTPS vulnerability	Yes
MEC vulnerabilities	Malicious apps attack MEC or UPF VN	No
	Resource competition among APPs Impact each other	No
	Overpowered management to third-party APP	No
Cloud vulnerabilities	Vulnerabilities of open source software is exploited.	No
	Unauthorized resource using and data reading.	No
	Difficult to locate problems with Multi-vendor integration.	No
	Eavesdropping or tampering with application layer communication content through virtual network.	No
Slicing vulnerabilities	Unauthorized access between slices or UE access to unauthorized slices.	Yes
	Resource pre-emption between slices leads to excessive resource consumption.	Yes
	Unauthorized slice O&M.	Yes

A more precise list of mitigating measures (in connection to Question 9 above)

Main vulnerabilities (as identified in table above)	**Existing mitigating measures**	**Effectiveness (LOW/MEDIUM /HIGH)**
Air interface: theft/tampering of user data and information on air interface	The encryption algorithm uses a 128-bit key. IMSI encryption is added to protect user privacy. Integrity protection is added to the user plane. The above is specified in 3GPP TS 33.501.	HIGH
Air interface: deny user access due to DDoS	gNodeB shall have the air interface data flow control mechanism to defend against distributed denial of service (DDoS) attacks launched by 5G terminals from the air interface.	HIGH
Air interface: illegal access to the network by unauthorized terminals on air interface	5G provides 5G-AKA authentication mode. The AUSF performs an authentication on the network access. For the details of 5G-AKA authentication processes see 3GPP TS 33.501.	HIGH
Air interface: false base station	Bidirectional authentication is performed between the UE and the network to prevent the existence of rogue base stations. IMSI encryption is added to prevent IMSI catching from pseudo base station.	MEDIUM
Air interface: trigger terminal fallback to 2G	Follow standard defined by 3GPP WG SA3.	HIGH
Internet security: leakage or tampering of user data during transmission	Should be guaranteed by application layer.	N/A
Internet security: spoofing network applications	Should be guaranteed by application layer.	N/A
Internet security: denying data services due to DDoS on Internet	Should be guaranteed by application layer.	N/A
Internet security: unauthorized access to exposure APIs	API access control.	HIGH

Roaming: leakage or tampering of user data during transmission	SEPP encrypt and protect the data integrity through TLS protocol.	HIGH
Roaming: forgery transfer operator and service rejection	Bidirectional authentication via TLS prevents fake NFs from accessing the network.	HIGH
Roaming: legacy signalling protocols (SS7, Diameter) manipulation	Security Edge Protection Proxy (SEPP).	HIGH
LI: illegal interception gateway access	Authentication based on IPSec or TLS.	HIGH
LI: leakage of the intercepted target ID	Encrypted target ID.	HIGH
LI: interception data leakage due to attacks from interception port	LI transmission encryption.	HIGH
5GC/MEC and 5G RAN: data eavesdropping on N2/N3 interface	IPsec is used between gNodeB and 5GC to ensure security.	HIGH
5GC/MEC and 5G RAN: data tampering on N2/N3 interface	IPsec is used between gNodeB and 5GC to ensure security.	HIGH
5GC/MEC and 5G RAN: unauthorized access on N2/N3 interface	IPsec is used between gNodeB and 5GC to ensure security.	HIGH
Software and hardware: unauthorized access to equipment via a physical interface	Indoor gNodeBs are often located in equipment rooms with door locks to protect them against illegal intrusion. Outdoor gNodeBs are housed in cabinets with locks and door status sensors. gNodeBs allows to disable the not used physical ports, including such as serial port, USB port and local Ethernet port.	HIGH
Software and hardware: unauthorized operations on NEs	gNodeB and 5GC NEs shall support access control basing on access rights of users to prevent unauthorized operations.	HIGH
Software and hardware: unauthorized software replacement or malicious software implantation	gNodeB, 5GC and EMS shall support digital signature to ensure software integrity before installation. Mandatory access control is implemented for the critical resources on gNodeBs. Access control policies are also configured to ensure that the access of processes to resources complies with the minimum privilege principle. This prevents privilege escalation and other forms of unauthorized access to resources.	MEDIUM
Data: locally stored confidential information is stolen or tampered with, such as keys, and user context information.	Access control. Encrypted storage. Storage backup. O&M logs and audit.	HIGH

Data: user privacy information is stolen or tampered with, including subscription data and CDRs.	Least processing of user privacy information. Access control. Encrypted storage. Storage backup. O&M logs and audit.	HIGH
Data: unauthorized access to user plane data from other planes.	Access control. 3 plane isolation: data plane, signalling plane and O&M plane.	HIGH
OM: unauthorized access	EMS with gNodeB and 5GC NEs shall support RBAC-based Identity Management to authenticate user access.	HIGH
OM: password cracking and leakage	NEs support the functionality including such as password complexity and login management to prevent password cracking. Password shall not be stored in clear.	HIGH
OM: malicious operations by authorized users	Administrators can monitor the online/offline status of local O&M users of the eNodeB. Administrators can monitor operations of local O&M users. Administrators can force O&M users to log out of the eNodeB.	LOW
OM: log deletion/tampering	gNodeB and 5GC does not provide any interface or command for modifying logs or deleting log files. That is, any person (including the gNodeB administrator) cannot delete log files from or modify logs on the NEs.	LOW
OM: sensitive O&M data tampering/leakage	TLS is used for protecting data transmission between NEs and EMS.	HIGH
OM: malware implantation	gNodeB, 5GC and EMS shall support digital signature to ensure software integrity before installation. Mandatory access control is implemented for the critical resources on gNodeBs. Access control policies are also configured to ensure that the access of processes to resources complies with the minimum privilege principle. This prevents privilege escalation and other forms of unauthorized access to resources.	MEDIUM
OM: web attack (e.g. SQL injection)	The web server identifies and denies invalid requests by checking requests against the whitelist before user login and checking the request validity based on information, such as the client IP address, session ID, and token, after user login. The web server checks the validity of the parameter type or format, such as the data length and data range, SQL syntax entered on the web client. Only the data filtered and standardized by the system is processed in the system or transferred to service module for further processing.	MEDIUM
SBA: DoS deny NRF to register and discover	NRF access authentication, overload control.	HIGH

SBA: attacker imitate NFs to access unauthorized data	NRF access authentication, overload control.	HIGH
SBA: eavesdrop and tamper data among NFs	SBA encryption by TLS.	HIGH
SBA: attack based on the existed HTTPS vulnerability	HTTPS vulnerability hardening.	HIGH
MEC: malicious apps attack MEC or UPF VN	Hardware isolation deployment Security zone isolation (vFW).	HIGH
MEC: resource competition among apps impact each other	Flow control. Hardware isolation deployment. KPI monitoring.	HIGH
MEC: overpowered management to third-party app	O&M logs and audit. Permission control, separation of operation and audit rights.	HIGH
Cloud: vulnerabilities of open source software is exploited.	Continuous detection and hardening of open source software.	MEDIUM
Cloud: unauthorized resource using and data reading.	Resource isolation. Permission control.	HIGH
Cloud: difficult to locate problems with multi-vendor integration.	SSO avoid frequent switchover of multiple management systems. Unified certificate management ensures certificate mutual trust between different vendors and improves certificate replacement efficiency. Operation monitoring platform enable big security data and correlation analysis.	HIGH
Cloud: eavesdropping or tampering with application layer communication content through virtual network.	Access control and encrypted storage. Encryption of key data transmission between VMs. Secure deletion.	HIGH
Slicing: unauthorized access between slices or UE access to unauthorized slices.	Access control. Slice ID verification. Access statistics monitoring.	HIGH
Slicing: resource pre-emption between slices leads to excessive resource consumption.	Slice flow control and user traffic limiting in slices Slicing resources reservation. KPIs monitoring (such as throughput and delay).	HIGH
Slicing: unauthorized slice O&M.	Separated O&M for system and slice. O&M audit.	HIGH

Annex- Example of a more detailed threat categorisation applicable to Software Defined Networking (source: ENISA SDN 5G threat landscape report) - for possible reference in the context of the national risk assessments.

- ***Nefarious activity/abuse***: This threat category is defined as "intended actions that target ICT systems, infrastructure, and/or networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target"

- ***Eavesdropping/Interception/ Hijacking:*** This threat category is defined as "actions aiming to listen, interrupt, or seize control of a third-party communication without consent"

- ***Physical attacks:*** This threat category is defined as "actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection"

- ***Damage:*** This threat category is defined as intentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness"

- ***Unintentional Damage:*** This threat category is defined as unintentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness"

- ***Failures or malfunctions:*** This threat category is defined as "insufficient functioning of an (Internet infrastructure) asset".

- ***Outages:*** This threat category is defined as "unexpected disruptions of service or decrease in quality falling below a required level"

- ***Disaster:*** This threat category is defined as "serious disruption of the functioning of a society"

- ***Legal:*** This threat category is defined as "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law"