BEREC
Body of European Regulators for Electronic Communications

BoR (23) 180

BEREC Report Secure 5G Networks

5 October 2023

Contents

1 Executive summary

In 2023 the BEREC surveyed European markets through questionnaires. The objective was to understand the present status of resilience and security in electronic communications networks within the participating countries. The survey, prepared by BEREC in collaboration with ENISA, the Commission, and the NIS CG, comprised two questionnaires—one for National Regulatory Authorities (NRAs) and another one for operators.

This report presents the results of the analysis of the responses received from the participating NRAs and operators, mainly within the EU, but also from a small number of non-EU countries. As an outcome from the results obtained, there is a number of possible issues that could be considered for further investigation.

Topics covered in the survey and the main findings:

- **Technological challenges**

  A) The report examines the role of NRAs in the cybersecurity ecosystem and their regulatory powers. The findings reveal diverse viewpoints among NRAs, with the majority asserting that additional powers are not required to reinforce their roles and regulatory authority. The report emphasizes the consensus on addressing cybersecurity and privacy concerns, while also underlining the importance of coordinated collaboration with other relevant entities.

  B) The second chapter of this report is focused on comprehending the technological challenges encountered by operators. It assessed the present status and future developments in the deployment of mobile networks across Europe.

  1) The results show operators still support various mobile technologies, with a shift towards 5G. Security concerns are addressed by using established standards and guidelines, highly respecting the ENISA Guidelines as well. Operators are actively taking steps to mitigate risks associated to different network functions, using a combination of international and national standards and guidelines.

  2) Regarding the coexistence of 5G Core and 4G Core, the majority of operators express confidence in the existing standards and guidelines for managing security risks. However, the findings underscore a consensus that both 5G Core and 4G Core will operate together for a prolonged period, necessitating thorough risk assessment and potential supplementary security measures. While a subset of providers seeks more precise directives for dual-core security, most are content with the current standards and guidance. The text also emphasizes the dynamic nature of network technologies and the continuous endeavours to ensure their secure adoption and functioning.

  3) The subject of Supplies Policy and the location of vendors' headquarters is another noteworthy aspect of this report. The findings underscore the complexity involved in vendor selection, as a growing number of operators are opting for multiple vendors while factoring in elements like geographical location, legal mandates, and security considerations. The recommendation stemming from the 5G Toolbox have led a

significant portion of operators to adapt their equipment vendor strategies to adhere to evolving regulatory and security benchmarks.

4) This report highlights the absence of a regulatory structure concerning substitution costs and emphasizes the necessity for measures that promote robust competition among vendors while addressing potential market outcomes. Interoperability testing is a prevailing practice, primarily managed by operators that rarely encounter significant obstacles. Although challenges are typically manageable, integration efforts might result in deployment delays. The overarching results underscore the critical nature of smooth integration and collaborative efforts between vendors and operators to ensure the effective rollout and functioning of 5G networks.

5) NVFV (Network Function Virtualization) and network slicing were interesting subjects of inquiry. The outcomes reveal that NFV enjoys extensive adoption, but security issues are acknowledged, notably the isolation of VNFs (Virtual Network Functions). While most operators haven't pinpointed risks linked to network slicing, certain potential risks have been identified. The focal point is on proactive risk evaluation and the establishment of effective security measures to guarantee the seamless implementation and operation of NFV and network slicing technologies.

6) Regarding the impact of regulatory demands on infrastructure deployment, operators hold diverse viewpoints, including their impact and the necessity for new legislative requirements for 5G security. Additionally, the importance of harmonizing EU legislation within the realm of 5G networks is underscored.

7) In the operators' technological challenges subchapter, the report reveals diverse perspectives on the security advantages of virtualization and cloud services. It also underscores the complex decisions and dilemmas faced by operators while embracing these technologies. Notably, the majority favouring private cloud usage reflects a prudent approach, emphasizing control and security in their network infrastructure.

- **Equipment replacement**

The majority of operators intend to keep 5G non-Stand Alone (non-SA) mobile technologies (4G/5G hybrid) in service for more than 5 years. The expected life cycle of 5G SA equipment in Core network and 5G RAN components is 5-10 years. For an equipment replacing strategy almost half of the operators are keeping with the current vendor. Others follow a range of different strategies such as putting in place network segmentation, replacing equipment using a different vendor, switching to Open RAN or to follow a different approach.

2 Introduction

In 2022, BEREC examined the Recommendations put forward by the European Court of Auditors (ECA). In the BEREC report on ECA Audit Recommendations for 5G Cybersecurity BoR (22) 197 issued in December 2022, BEREC assessed these Recommendations, aiming to present its perspectives and suggestions for forthcoming actions to assist the Commission in their implementation. Throughout this analysis, BEREC identified areas where it could offer support to the European Commission through a data gathering exercise, which is now outlined in this report.

In 2023 the BEREC conducted a survey through a questionnaire in European markets to gather pertinent information. The main objective was to gain deeper insights into the present status of resilience and security in electronic communications infrastructures and networks within the EU and other participating countries. Additionally, this initiative aimed to identify potential areas that warrant increased focus in the future. The survey which was prepared by BEREC and cooperating parties such as ENISA, the Commission, and the NIS CG, consisted of two questionnaires. One questionnaire was prepared for National Regulatory Authorities (NRA) and the other one for providers of Electronic Communications Networks and Services operating in the European market (operators). The questionnaires were divided into two (NRA) or three (operators) sections, each addressing a different field of interest. The primary objective for consulting both NRAs and operators was to gain a comprehensive understanding of the implementation of the security measures. This endeavour should enable the identification of potential gaps that may demand further attention and reveal areas where additional support to operators and NRAs would be necessary to enhance the resilience of communication networks. Some of them are presented in this report.

This report is based on the analysis of the questions related to the security of the 5G networks from both questionnaires as indicated in the table below. The remaining questions of the survey, that relate to the resilience and dependencies on other infrastructures, will be analysed in a second report that should be presented and adopted by BOR in December 2023.

Questionnaire for the NRA:	
Technological Challenges:	Dependencies on other infrastructures:
Questions in scope of this report: 1-5	Questions in scope of this report: -
Questions that will be analysed for the second report: 6-13	Questions that will be analysed for the second report: 1-25

Questionnaire for the Operators		
Technological Challenges:	Equipment Replacement:	Dependencies on other infrastructures:

In scope of this report: 1-20	In scope of this report: 1-4	In scope of this report: -
The questions that will be analysed in the second report: 21-34	The questions that will be analysed in the second report: -	The questions that will be analysed in the second report: 1-27

This report focused on 5G networks deployment status, investigated 5G security risks and the equipment replacement cycle. Some aspects of existing restrictions on 5G equipment from high risk vendors are presented as well.

The two questionnaires, as per Annex 1, were sent to all 37 BEREC members' NRAs (adhere: NRAs) including the 27 EU Member States (MS). One questionnaire was prepared for NRAs and the other one for the operators offering services in BEREC member countries. The information collection period was from April 14th to May 26th 2023. With some individual extensions given a deadline of June 14th, the majority of replies were sent to BEREC via NRAs. Answers from operators were collated nationally and were anonymised by respective NRAs before they were sent to BEREC. As a result, BEREC collected 123 answers from operators and 30 from BEREC members (NRAs). The list of countries that participated in the Survey is attached to this report in Annex 1.

BEREC had been working closely with ENISA, the NIS CG, and the Commission during the questionnaire development phase with close cooperation continuing in the future after this report has been completed.

3 Results

3.1 Technological Challenges for NRAs

3.1.1 The need to strengthen the role of NRAs

Question 1 **-** Do you believe that it is necessary to further strengthen the role of national authorities with the adoption of strategic and/or technical measures and/or supporting actions?

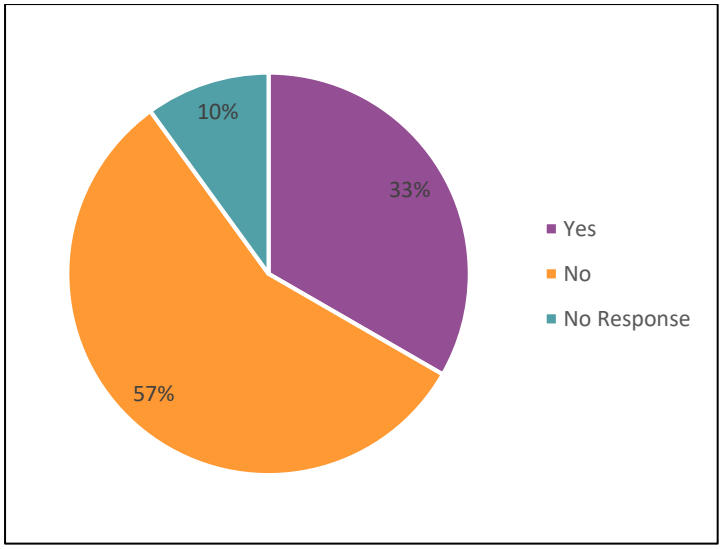

Figure 1 – The need to strengthen the role of NRAs.

There were 27 (out of that 24 coming from the MSs) responses to this question, 17 (63%) NRAs responded that they did not believe it was necessary to further strengthen the NRA roles in their jurisdictions and 10 (37%) believed that it was necessary. Of those who said that there was a need to further strengthen their roles the following additional details were provided:

One NRA responded that given the emerging complexities of network traffic and the potential need to ensure the delivery of critical services, NRAs should be granted the regulatory power to mandate, under specific and controlled circumstances, the prioritisation of certain traffic (e.g. essential public services, emergency communications, or other high-priority applications as deemed necessary for national security, public safety, or economic stability) within 5G networks. This should include the powers to allow the NRA to carry out necessary technical testing with the operators. They also suggested that, for transparency some oversight of this prioritisation should be established. Such prioritisation should be subject to periodic review and public oversight to maintain trust and accountability. Other NRAs commented that the areas related to cybersecurity and privacy need further strengthening, or that NRAs should become a Single Point of Contact and coordinator between authorities, institutions and other relevant parties including operators, and exposed the need for strengthening further the role in the area of digital infrastructure and the partnership with BEREC, ENISA and the NIS CG.

While the majority of NRAs did not believe that further strengthening of the role of the NRA was needed, those who believed that it was, provided some comments that would benefit from further study.

Question 2 - If Yes, to 1, should this include additional regulatory powers for national authorities, to be able to use more effective ex-ante powers to restrict, prohibit and/or impose

specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment?

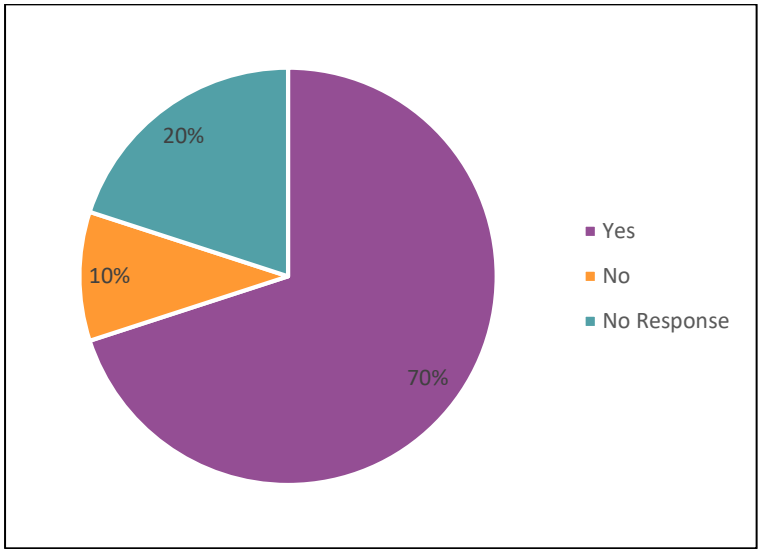

Figure 2: Need for more ex-ante powers in relation to supply deployment and operation of 5G equipment?

This follow-up question was related to the 10 NRAs that answered "Yes" to the previous question. The additional details they provided were as follows:
One NRA responded that it would strengthen security if the NRA had the power to require the operators to conduct specific risk assessments for newly identified risk(s) by the NRA and decide on appropriate security measures against that risk, which would be part of the NRA's enforcement. New risks could relate to the supply chain, warfare etc. This could also have the potential to give NRA's the power to require an operator to implement specific measures based on the risk assessment. NRAs should be able to require operators to regularly report on their 5G network security practices and any identified vulnerabilities.

Other NRAs responded that they should be given the power to impose obligations in this area and control implementation, mentioning ex-ante powers for the NRA to set requirements for the supply, deployment and operation of the 5G network equipment for the implementation of the technical measures deriving from the 5G Toolbox.

3.2 Technological Challenges for Operators

3.2.1 Support of mobile technologies in operators' networks

Question 4 - Do you support the following technologies in your network?
Do you support 2G?
Do you support 3G?
Do you support 4G?
Do you support 5G (4G core)?
Do you support 5G Stand Alone (SA)?

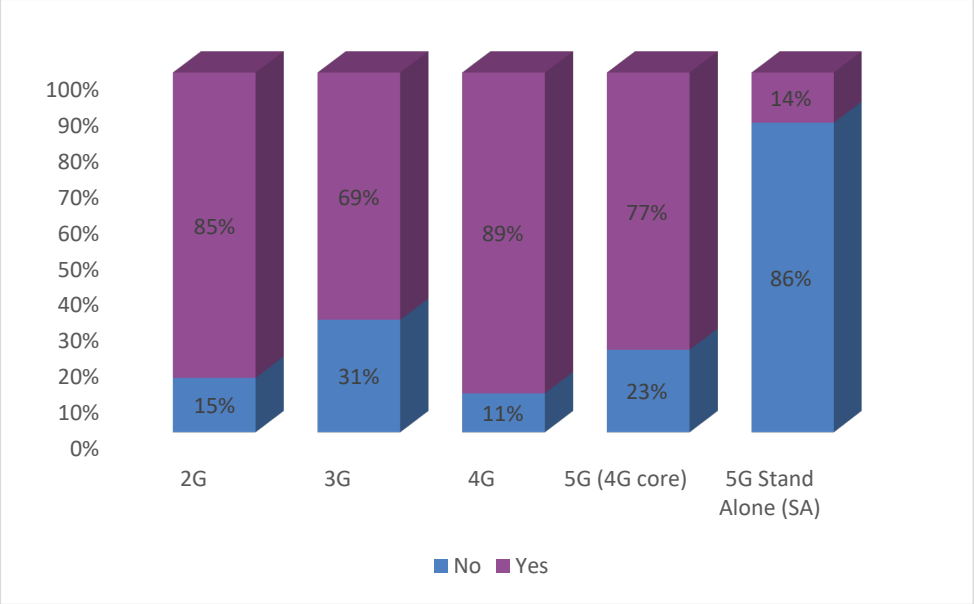

Figure 3 – Technologies supported

When asked about the technologies that they support, the operators stated, with a majority, that they provide 2G (85%) and 4G (89%) networks, while 3G are supported to a lesser extend at 69%. There were 77% of operators that support 5G through a 4G Core and 14% that already support 5G Stand Alone (SA).

Question 5 - If you support 5G what percentage is Stand alone?

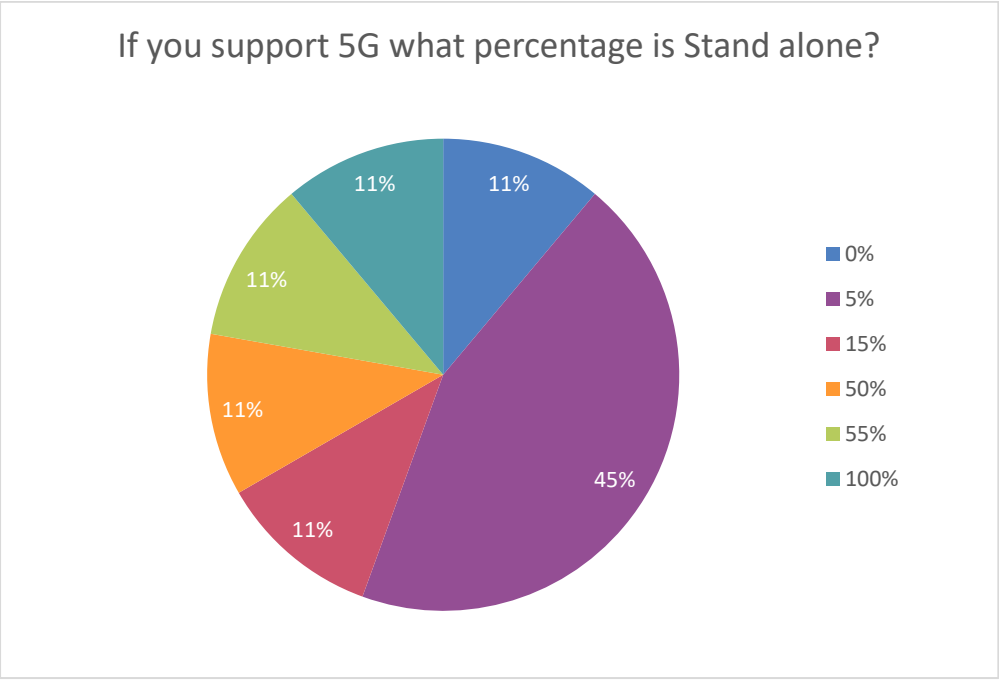

Figure 4 – Percentage of 5G SA.

The 9 operators that have answered they support 5G networks were also asked about the percentage of SA deployment. For two thirds this stays below 20% while 8% of the operators have a fully 5G SA network.

Question 6 - If your network has a cloud based 5G SA core, which network function has the highest level of security risk?

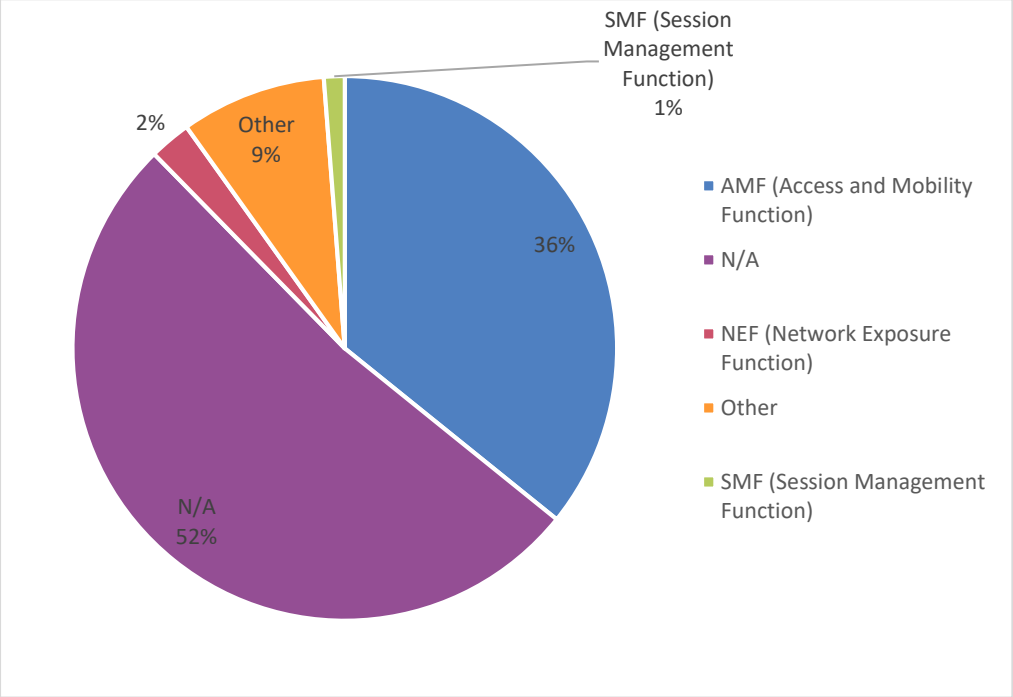

Figure 5 – Network function of the highest risk.

The following question was also addressed only to those operators that own 5GSA networks and was meant to identify the network functions that are considered as having the highest level of security risk. 81 operators provided the answer. The Access and Mobility Function (AMF) is with 36% mentioned as the network function with the highest level of risk. Only 3% operators mentioned the Network Exposure Function (NEF) or Session Management Function (SMF).

Question 7 - Where are those cloud based functions located?

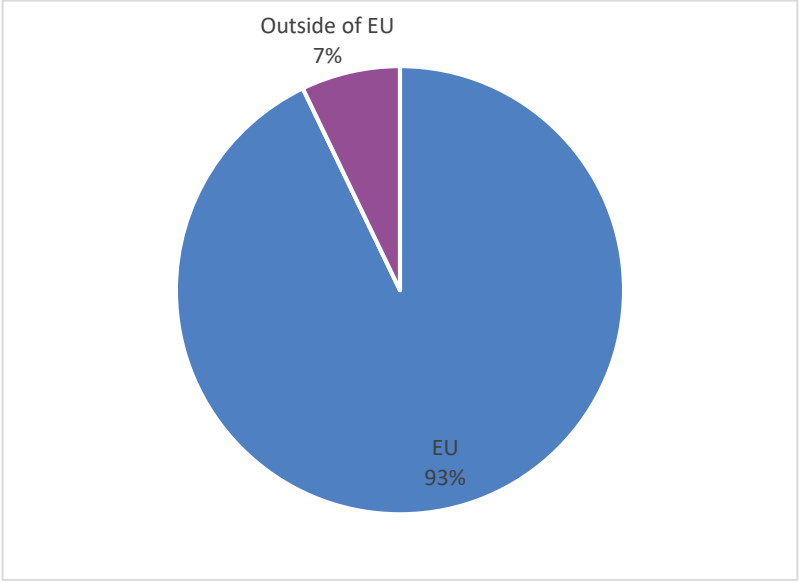

Figure 6 – Locations of cloud based functions

28 of the operators that have 5G SA networks provided the answer. All operators that are EU based answered that their cloud based functions are located in EU. 2 operators from non EU countries answered that they are located outside of the EU.

3.2.2 Mitigation measures against the identified risks to the Network Functions

Question 8 - When you put in place mitigation measures against the identified risks to the Network Functions listed for the cloud based 5G SA core, do you follow standards and guidance from?

- 3GPP/ETSI
- ENISA
- GSMA
- ISO or other standards
- National guidelines
- Other international standards

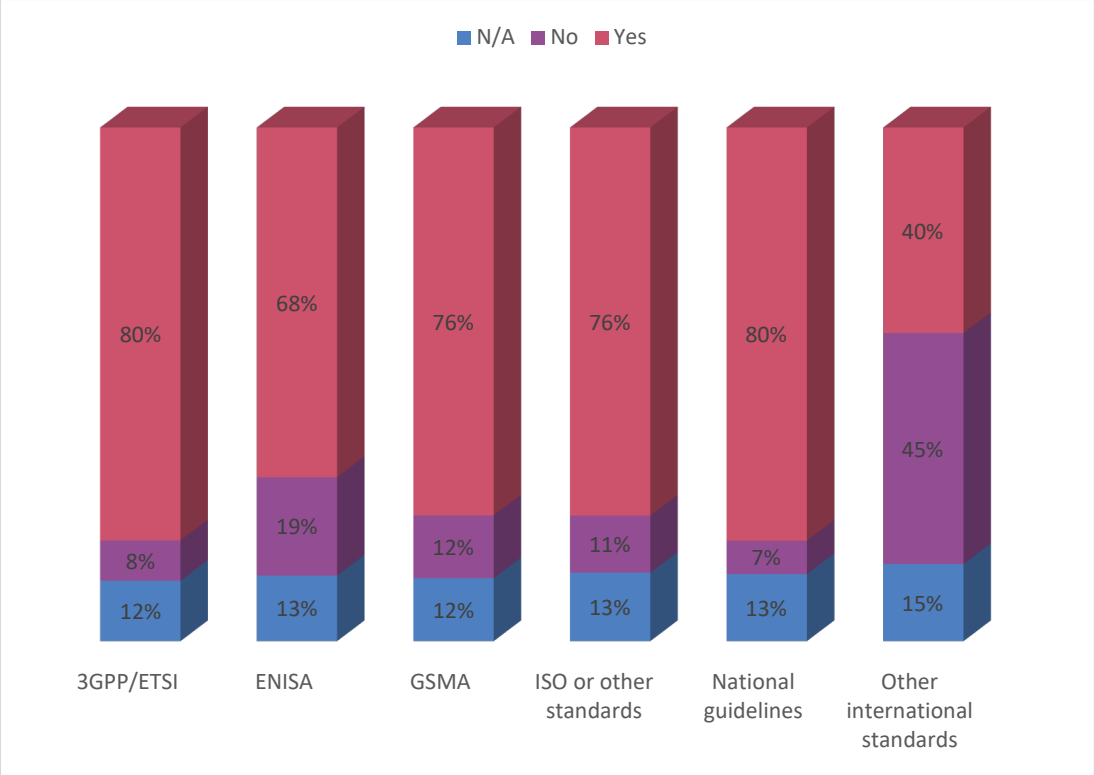

Figure 7 – Standards and guidance for cloud based 5G SA Core.

Out of 51 operators that answered this question the majority follows standards and guidance when putting in place mitigation measures. The 3GPP/ETSI standards and national guidelines are both used by 80% operators. Also the GSMA and ISO or other standards are used by more than 75% of the operators. The ENISA guidelines are followed by nearly 70% of operators. 40% of them also stated that other international standards are used and the details related to them were provided in the next question.

When asked about some details, operators mentioned the 5G Toolbox, 5G National Guidelines from the cybersecurity authorities and internal security documents and standards.

3.2.3 Co-existence of 5G core along with 4G Core and additional risks

Question 9 - For how long do you expect that 5G core will co-exist with 4G Core?

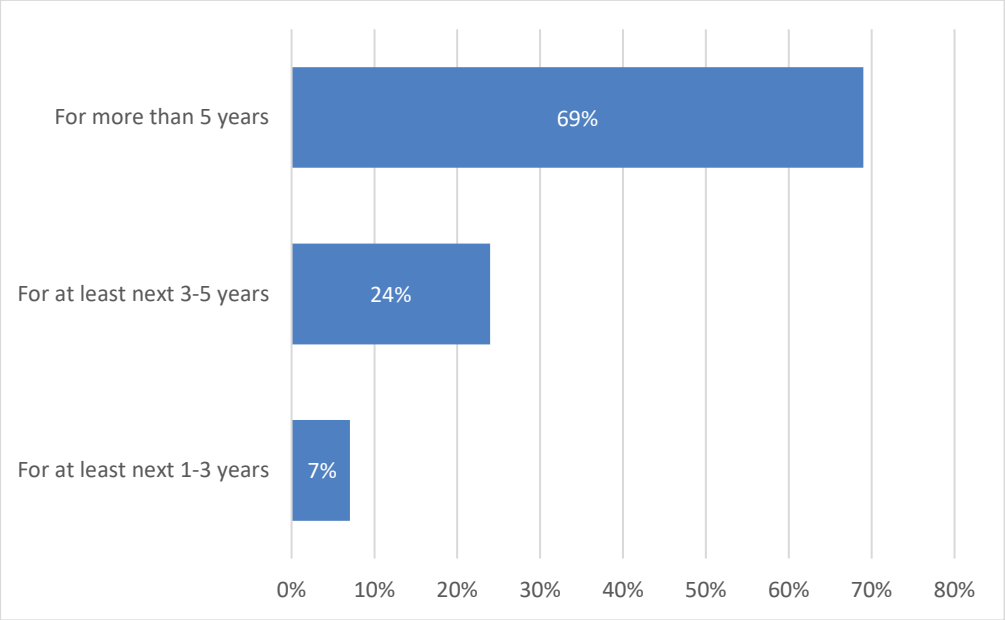

Figure 8 – Length of time 5G core will co-exist with 4G core.

Among the 71 respondents, the majority expects that 5G core will co-exist with 4G Core for more than 5 years.

Question 10 - In your view, are there additional risks related to dual core (4G/5G)?

According to the answers received to this question (74 in total), 35% of the providers identified additional risks associated with the implementation of a dual-core system, while, the majority, constituting 65% of the providers, disagreed with the statement and think there are no additional risks. Some of the operators that answered affirmatively, indicated that additional risks might come from: diameter signalling, hosted SEPP, container based infrastructure or even interoperability challenges.

Question 11 - Did you need to take additional security measures when implementing dual core (4G/5G)?

39% of the operators (out of 70 in total) confirmed that they need to take additional security measures when implementing dual core. The remaining 61% said they did not need to take additional security measures.

Some of the operators also provided additional information on this question. One operator commented that appropriate network segregation and isolation has been applied and complemented with security hardening at network function (NF) level. Others stated that

security policies are currently in line with 5G security recommendations, while others will follow their business continuity plans.

Question 12 - Is there a need for additional standards or guidance related to the issue of security of dual 4G/5G core?

When talking about additional standards and guidance, 28% of the operators (of a total of 75) expressed their belief that there is a requirement for further documents, specifically focused on addressing the security aspects of dual-core systems. But the majority, accounting for 72% of the providers, were of the opinion that the current standards and guidance available for dual-core security were comprehensive and adequate.

3.2.4 Supplies Policy – Vendors' Headquarters location

Question 13 - How many suppliers of 5G Core equipment (e.g. AMF, NEF, SMF) are you using?

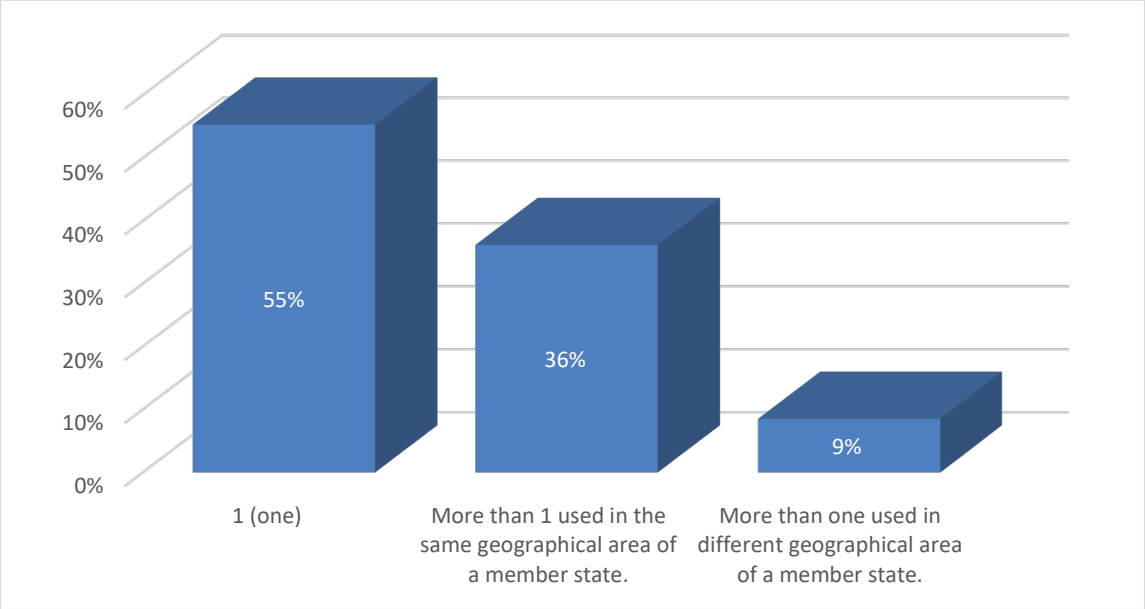

Figure 9: Number of 5G core equipment suppliers used.

Among 47 operators that provided the answer more than half of the operators that currently operate or plan to operate a 5G network in the future (55%) use one vendor of 5G core equipment (e.g. AMF, NEF, SMF). Almost half are using the multi-vendor strategy (Strategic Measure 05 of the 5G Toolbox) approach in different ways**:** 36% indicated that they use more than one vendor in the same geographical area, while 9% use more than one vendor in different geographical areas of a MS. Some operators use different vendor for UDM and SCP functions and another operator uses different vendors for different core functions. Some indicated to use one for SDM and core (AMF, NEF, SMF) and another vendor for Signalling (NRF, SCP). Some are using different vendors for different 5G Core Network Function per

market but more than one vendor across multiple 5G Core functions. Some mentioned current planning to develop 5G core network and were considering using more than one vendor.

More than half of operators currently have one vendor for 5G core equipment, however a significant percentage (41%) use more than one vendor.

Q14 - How many of those vendors in the previous question are headquarter-based in:
EU
USA
China
South Korea
Japan
Other, please specify in comments column

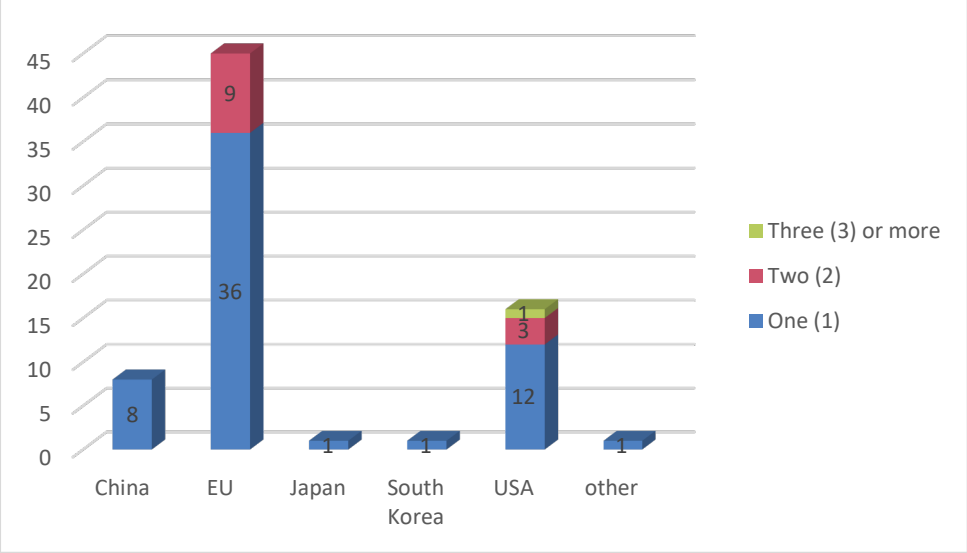

Figure 10: Number of vendors per country of headquarters.

Most of the operators responded that they use vendors from the EU (36 operators indicated one vendor and 9 operators two EU vendors). 16 operators are using vendors from the USA (12 operators are using one, 3 are using two vendors and one operator is using three or more vendors from the USA). Eight operators, among them 4 EU based, are using a single vendor from China and one operator is using the vendor(s) from Japan and another from South Korea. Some further explanations were given by the operators mentioning using one EU vendor and being currently in the process of selecting vendors for other features meaning outside CORE. One operator mentioned to be in the process of migration from China based Core vendor to EU based and another one mentioned the plan to use an EU vendor.

Most of the operators (45) use vendors located in the EU, while vendors from the USA (16) are also being selected. Less operators (10) use vendors headquartered in Asian countries.

Question 15 - Did you need to change your plans for equipment vendors due to any decisions at the national level based on the legislative requirements arising from the 5G Toolbox?

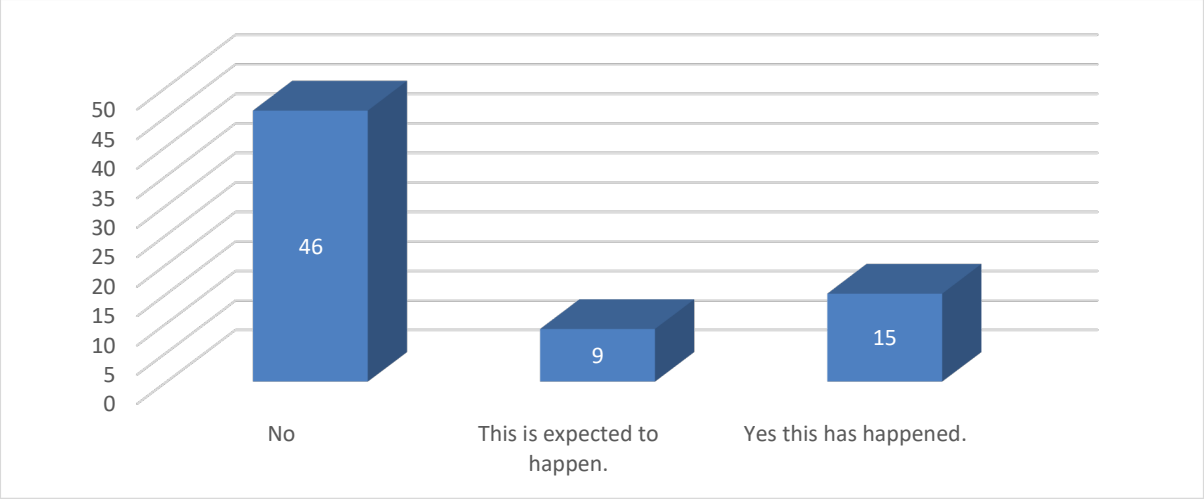

Figure 11: Change of plans on equipment vendors due to a national decision.

Most of the operators (66%, 46 out of 70 in total) responded that they did not have to change their plans regarding equipment vendors following decisions related to the 5G Toolbox. 15 operators out of 70 in total (21%) responded that they were obliged to make changes while 13% answered that they expect this to happen in the future. Some further explanations to this question were provided by individual operators. Two operators mentioned the need to change supplier due to a law to avoid high risk vendors. One operator responded that they have to consider the location of the headquarters of vendors in case of technological upgrade tenders. One operator answered that they have to change their plans for the access network. One operator responded that they had a veto for using a Chinese vendor for the 5G SA core network. One operator answered that relevant security measures were taken before the implementation of the 5G Toolbox. One operator indicated that even though there is no legislative requirement yet, they take notice of the relevant security measures. One operator said that 5G Core vendor selection was made before the 5G Toolbox was released, although the risk was evaluated in the process of vendor selection. One operator stated that even though there is no final decision on a law related to vendor headquarter requirements, it will align to the group decision to change the Core vendor. One operator stated that even though there is no final decision on a law related to vendor headquarter requirements, it will align to the group decision to change the Core vendor.

A not negligible percentage of the operators that responded to the survey (21%), stated that they had to change their plans in relation to the equipment vendor selection following the legislative requirements stemming from the 5G Toolbox. On top of this, 13% of the operators are expecting this to happen. The majority are mentioning the Core equipment.

3.2.5 Regulation Framework

Question 16 - Is there a framework in place that regulates the substitution cost that you can rely on in case you would need to replace your equipment before its expected life cycle expires?

74 out of 76 operators who responded to the question said that there is no framework on the substitution cost. Only 2 respondents indicated that there are relevant regulatory provisions in

place. One operator answered that this is included in its' Business Continuity Plans (BCP). One operator answered that there is no such framework, however this was proposed when adopting legislative measures in relation to the national implementation of the 5G Toolbox and it was finally not adopted by the government. The operator proposes that an assessment of the impact on the entities affected should always be done whenever an administrative ban on existing equipment is introduced. If this happens before the life cycle of the equipment expires, this should involve compensation for the operator through mechanisms compliant with state aid rules. Also, the consequences on the market competition should be considered when excluding a vendor from the market, as there would be limited number of vendors available in that case. Measures might need to be taken in order to prevent possible price increase and inappropriate delivery time and conditions. It should be ensured that the implementation of the 5G network will be done within an environment with healthy vendor market competition and not allowing non-market behaviour of certain vendors. One operator responded that there is a provision in the legislative framework on a transitional period to comply with additional security measures.

There is no regulatory framework regarding the substitution cost for equipment before the life cycle expires based on the answers from 76 operators.

Question 17 - Have you performed some interoperability testing for the equipment from different vendors?

Just over the half of the operators (51%, 37 out of 73 in total) have performed testing in order to determine the interoperability of equipment, while 49% replied that they have not performed relevant tests. Some further information was also provided. One operator plans to perform interoperability tests in the future, two operators responded that interoperability tests are performed when needed, one operator answered that interoperability tests are in general performed in group level and another one stated that even though 5G SA is not yet implemented, tests were already performed. One operator explained that there are vendors that conduct their own interoperability tests and another one responded that interoperability tests were performed between different Core functions and between RAN and Core.

Approximately half of the operators responded that they perform interoperability testing for equipment from different vendors, however the other half said that they have not done so yet.

Question 18 - Have you found any interoperability issues that you consider significant enough to prevent or limit their deployment in your network?

Most of the operators (90%) answered that they have not encountered significant interoperability issues. Only 8% of the operators answered that they experienced such issues. Further explanations were provided by the operators responding to this question. One mentioning no interoperability issues, but experienced significant delay in deployment or vendors not being sufficiently prepared to Transport Layer Security (TLS) implementation on the Service Based Interface (SBI) causing slower integration to the mobile network operator. One operator found that there are some 5G functions that have to be deployed with the same vendor. One operator stated that they have performed interoperability testing for the

situation of using virtualized / cloud-based network functions from different vendors, not to any extent verification of all vendors and all functions, but limited to three vendors and only few functions taken from vendor #2 and #3). The result was that such interoperability is possible, but this is not "copy-paste" process and requires specific customisation and parametrisation and it needs active participation of the vendors. As of the current RAN solution, it should be noted that deployment of eNodeBs shall happen within (rather big) geographical clusters to assure predictable parametrisation for delivering proper quality of service, the statement on interoperability shall be read in the way, that interoperability of different 5G RAN with the core is assured, but current advancement of technology does not allow to make random geographical deployment of mixed radio solutions (i.e. it will not work properly when one will implement every second eNodeB from one vendor and another vendor).

Operators do not experience significant interoperability issues that would prevent or limit the deployment in the network, however significant delays are experienced due to the work required for the integration of the systems.

3.2.6 Network Function Virtualization

Question 19 - Do you use Network Function Virtualisation in your core network?

Most of the operators (83 in total) gave a positive answer while 15 of the respondents indicated that they do not use NFV.

In case of 5G Core, one mentioned it is based on Cloud-native Network Functions (CNFs) running in containers. Others are using NFV in 4G/Legacy Core or NFV in the IP Multimedia Subsystem (IMS) VoLTE Core Network. Two operators commented that they use NFV for their 5G non-SA networks as they don't currently have 5G SA.

Most of the operators use Network Function Virtualisation (NFV) in their core network.

Question 20 - If Yes to 19, what are the main security risk factors that you identified? Isolation of Virtual Network Functions Compromise of Host Kernel Compromise of Hypervisor Compromise of MANO Multi-tenant virtualization Administrator account compromise Other. Please specific in comments column

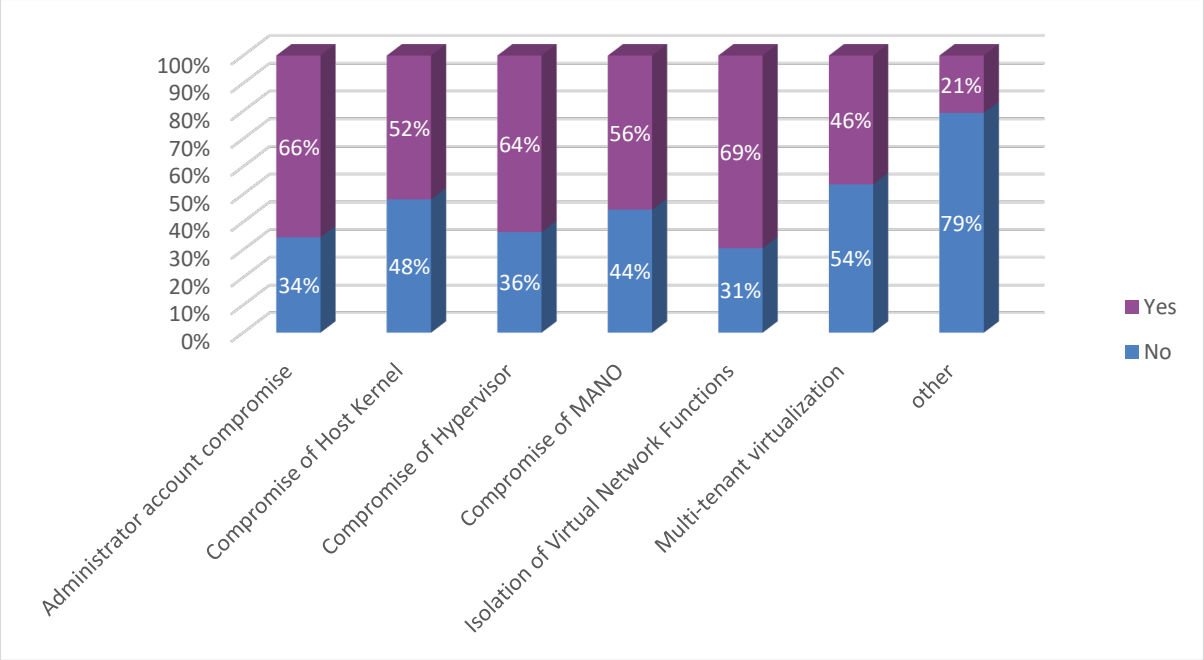

Figure 12 - Main security risk factors identified.

For this question, 60 operators in total provided responses. Isolation of Virtual Network Functions (VNF) was identified as a main security risk factor by most of the operators (41), followed closely with 38 for Administrator account compromise, Compromise of Hypervisor was 35, Compromise of MANO was 30, Compromise of Host Kernel was 28 and Multi-tenant virtualization was indicated by 26 operators. Other factors that were indicated by 6 of the respondents which were specified as the increased complexity to secure all layers.

Further explanations were given regarding the isolation of VNF. One operator stated that if VNFs are not appropriately isolated, and resources are not shared effectively, there is a risk of potential side channel attacks which enable an attacker to gather information about cryptographic secrets and use that information to induce faults. Another operator noted that they are using multiple platforms for different applications and their IP network has been heavily isolated.

Regarding the Compromise of Host Kernel one operator noted that since the kernel is shared among all containers on a host, a kernel breach can compromise all containers and the host itself used by the container engine. Therefore, the more applications on the host, the greater the denial-of-service attack risk. Regarding the Compromise of Hypervisor the hypervisor is fully aware of the current state of each guest OS it controls. It can view, inject, and/or modify information on the operational status associated with NFV. Access to status information can result in the ability to arbitrarily read and/or write the contents of memory, storage, key storage and other NFV operational aspects.

Regarding the Compromise of Management and Orchestration (MANO), one operator stated that since it is the framework with which the virtualized infrastructure, provisioning and automation of the network is managed, its compromise would cause damage to the entire infrastructure and the services it provides. Another operator noted that VNF orchestration as per ETSI MANO seems no longer applicable to an industry which has largely evolved to containers based on Kubernetes. Concerning the Multi-tenant virtualization, one operator noted the risks of incorrect resource allocation and lack of data isolation. With regard to the

administrator account compromise there was a comment that logging into an account with administrative privileges can give attackers access to all or most of the data on the infrastructure.

Two further general comments were made, one operator noted that, in general, virtual/cloud based implementations are creating different technological challenges compared to physical implementations, however existing technical standards of technology and cybersecurity, properly implemented in service provider environment are protecting networks, services and users from cyber threats. Another operator added for all options related to security risk factors that network operators should have holistic security plans, certified by ISO27001, that include element segregation, stateful firewalling, vulnerability management, penetration testing, etc.

Isolation of Virtual Network Functions, Administrator Account Compromise, Compromise of Hypervisor, Compromise of MANO, Compromise of Host Kernel, Multi-tenant virtualization all were identified as significant security risk factors by the operators. Apart from these security risk factors covered in the questionnaire, operators highlighted other factors as outlined in the text above.

3.2.7 Risks related to the network slicing

Question 21 - Have you identified any risks related to the network slicing?

Operators were asked about risks related to network slicing. The 69 answers provided revealed that network slicing is not yet widely commercialised. A significant majority of operators (50) stated that they have not identified any risks, while 17 operators acknowledged that they have identified some risks connected to the implementation of network slicing. Some of these also provided comments to support this. It was pointed out that some security risks associated with network slicing are documented by 3GPP in "TR 33.811, 33.813 and 33.874". Some operators identified the risks related to the situation when network Slice Data Theft and Tampering can occur even where physical network resource isolation is in place, malicious network functions in one slice may access services provided by other slices if there is no proper authorisation mechanisms between slices and access restricted data. It was also stated that excessive Network Slice Resource consumption can be an issue if the network resource management is not well performed, malicious users in one slice may request excessive shared network resources, resulting in resources being unavailable for all other slices. Some operators stated that they did not yet provide network slicing but identified theoretical risks and mitigation measures. One operator stated that network multi-slicing have not been implemented yet, but there are risk identified associated to the service implemented.

Most of the operators haven't yet identified any risks related to the network slicing. From the answers received it can be concluded that network slicing is not widely commercialised yet.

3.2.8 Regulatory demands as a limitation to deploy infrastructure

Questions 22 and 23 - Do you see regulatory demands as a limitation to deploy your infrastructure, according to best-practice IT- and cloud models?
If Yes to 22, please provide a brief description.

According to the answers received, a significant majority of operators (59 out of 77 in total) do not perceive regulatory demands as an obstacle for their infrastructure deployment. On the other hand, 18 of the operators indicated that they consider regulatory demands as a limitation in the process of deploying their infrastructure.

Some operators see further regulatory demands as a limitation to deploy their infrastructure, giving as an example the "limited vendor selection", or trustworthiness of the vendor. The regulatory frameworks for lawful interception and data retention do not allow operators to have core network infrastructure outside national borders, thus prohibiting centralised or regional core network infrastructure in one country serving customers in a different country.

The point was made that in general localisation requirements undermine the EU Digital Single Market and reduce operational effectiveness. Re-shoring of Network Operations Centres and Security Operations Centres creates significant problems for pan-EU industries by diluting or removing the advantages of scale and disrupting carefully tailored capabilities and operating models designed to ensure Critical National Infrastructure is resilient and secure.

One operator stated that limitations on vendor nationality could potentially lead to a longer time for market to get new technologies and in some cases to additional (higher) costs due to a reduced competition. Another operator stated that legislation and procedure in practice should be amended in order to provide easier and faster administrative processes for

construction of new base stations. They went on to state that according to EU Law all network elements need to be within the borders of the country in order for conduct supervision from the NRA, and public cloud solutions for network elements are not clearly defined. Another operator added that there are security related requirements, concerning aspects such as national autonomy, and other regulatory requirements (i.e. GDPR) that they must follow.

A significant number of the operators do not see regulatory demands as a limitation to deploy their infrastructure.

3.2.9 Need for new legislative requirements on certain aspects of 5G networks security

Questions 24 and 25 - Do you see the need for any new legislative requirements on certain aspects of 5G networks security?

If Yes, would it be due to the need for harmonising the legislation in EU?

Out of the 76 valid answers received to this question, almost 79% of them are stating that there is no need for further legislative requirements to be imposed, the remaining 16 operators are in favour of additional security requirements on certain aspects of the new networks.

Linked to this question, the operators were asked about the necessity to harmonize EU legislation and 11 out of the 16 that answered said that there was a need for better harmonisation.

The majority of operators believe that there are sufficient legal requirements and no further need for special aspects of 5G networks security.

3.2.10 Security benefits in utilising virtualisation and cloud services

Questions 26 and 27 - In deploying 5G SA, in your view, are there security benefits in utilising virtualisation and cloud services?
Please provide some details.

As obtained from the answers collected, there was an ambiguous view, with approximately half of the operators providing affirmative responses (28) while the other half providing negative responses (33). The lack of clarity in the responses suggests that there might be varying perspectives or uncertainties among the operators regarding the benefits of virtualization and cloud services.

Among the benefits that were mentioned there was Cloud APIs as it provides better visibility for security posture, dynamic resource consumption for test environment, disaster recovery and capacity boost, cloudified OSS platforms, service- software upgrades greenfield security, security by design high availability, faster recovery lifecycle accelerator, modularity of Core functions, lower hardware cost, easier maintenance and scalability, Network resilience, NRF (Network Repository Function) and AUSF (Authentication Server Function) that provide the

above benefits, scalability and flexibility, that simplified service deployments. The scalability and time-to-recover can be easily addressed in cloud native environments as well as automated response in case of incidents, service isolation, reduction of physical risks, centralized monitoring, TLS encryption, patch management.

Counterarguments mostly mentioned were that cloud services are not being yet ready as service for telco network functions. Naming bad accessibility and difficult and costly proper network separation from other cloud clients. Isolation of network functions as a vital importance was mentioned further and bringing all network functions onto a same Virtual Network Functions (VNF) / Cloud-native Network Functions (CNF) environment that bring security risks such as outage or compromise of the environment, which could lead to deterioration of the QoS and customer perception.

Some responses noted that implementing virtualisation can be challenging for smaller networks due to the complexity and increased attack risk surface compared to their dedicated hardware environment. This is possibly due to the resource and skills requirements to change to the virtualised environment. Among arguments in between there were different security considerations but not necessarily perceived as a benefit. Operators mention they are still looking at options for a 5G SA deployment and vendor selection and expect to learn from the RFI they are running. Monolithic single purpose HW/SW is less vulnerable from IT security perspective but has disadvantage for current and future development of software applications. Another point given was that while Virtualization and cloud services pose new security challenges and can increase the attack surface in the infrastructure layers, the ecosystem can benefit from existing widely used and mature cybersecurity solutions from the cloud-native/IT-world.

There is no clear position among the operators in favour nor against using virtualisation or cloud services in respect to the security benefits. Approximately one half sees security benefits in deploying 5G SA mostly due to scalability. The other half sees increasing security risks due to virtualization and cloud services.

3.2.11 Cloud-based architecture

Question 28 - With regard to your cloud-based architecture current or planned, will you use:

- Public Cloud
- Private (own) Cloud
- Hybrid Cloud
- Multi Cloud Strategies

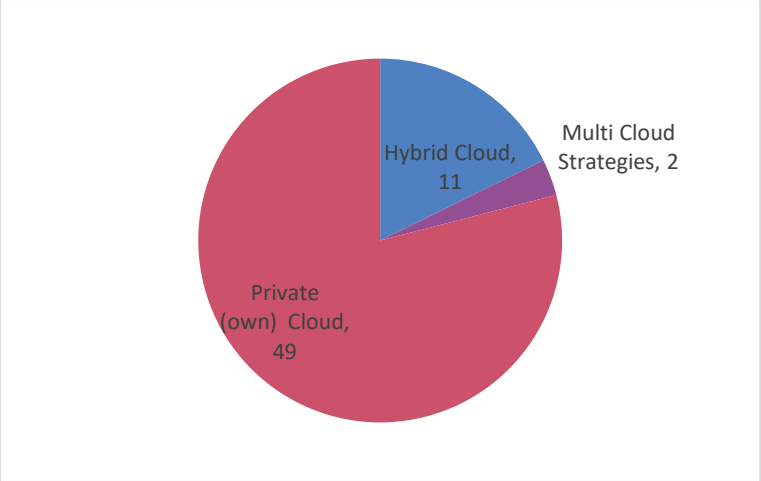

Figure 13 – Type of Cloud-based Architecture.

49 out of 61 operators that responded to this question use Private (own) Cloud. Eleven operators use Hybrid Cloud and two are using Multi Cloud strategy.

The majority of operators use their own private cloud followed by Hybrid Cloud and Multi Cloud Strategies. None of the operators who responded use only Public Cloud.

3.2.12 Equipment replacement

Replacement cycles for equipment are of high relevance from a cybersecurity point of view. Each replacement cycle (in principle) allows network operators and service providers to implement fundamental changes not only in technology and security-wise but also regarding the vendors used. With the issue of high risk vendors becoming an increasingly important matter, replacement cycles are perfectly suited to review the current set-up and take decisions on vendors and service partners.

Question 29 - How much longer do you expect to keep 5G non-SA mobile technologies (4G/5G hybrid) in service?

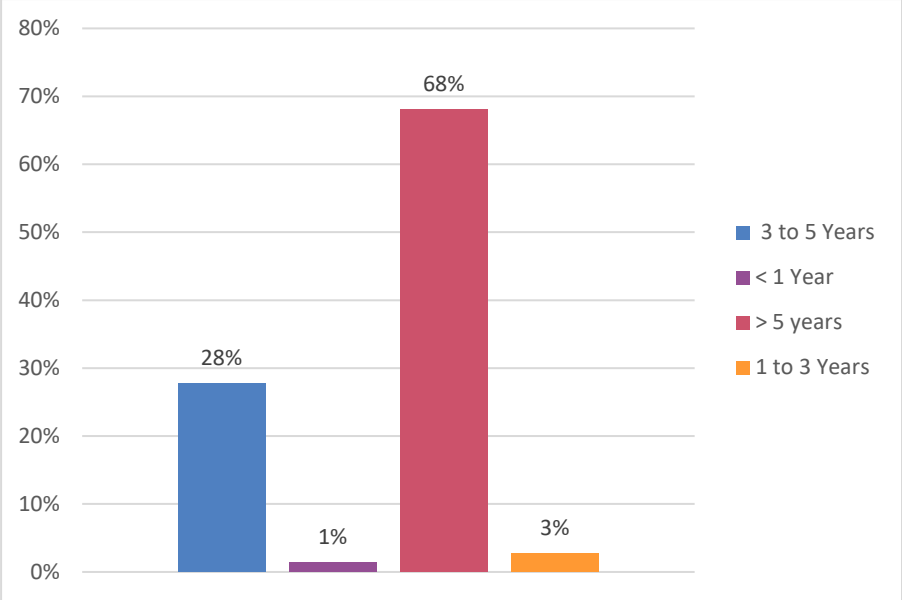

Figure 14 – Length of time for keeping 5G non-SA.

The implementation of 5G typically follows a path from a 5G non-SA implementation using 4G in the Core Network and 5G in the RAN to a 5G SA implementation ultimately using 5G in both Core and RAN. The question regarding the duration of 5G non-SA technology to be in use is of relevance as the full set of advanced 5G features is only available in 5G SA.

The majority of the responding operators (49 out of a total of 72) expects to keep 5G non-SA mobile technologies (4G/5G hybrid) in service for more than 5 years.

Question 30 - What is the expected life cycle of 5G SA equipment in your Core network?

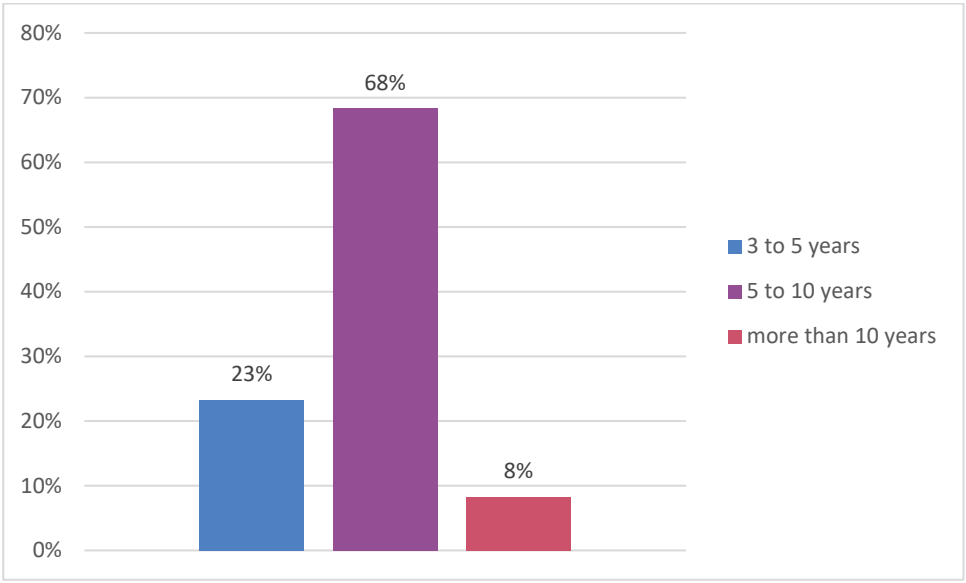

Figure 15 – 5G SA core equipment life cycle.

With regard to 5G SA implementations, operators were asked about the expected life cycle of the 5G SA equipment in their Core network. Similar to the previous question, a large majority of operators (67%) expect a 5G SA lifetime in the Core Network between 5 to 10 years.

Question 31 - What is the expected life cycle of 5G equipment for the RAN components in your network?

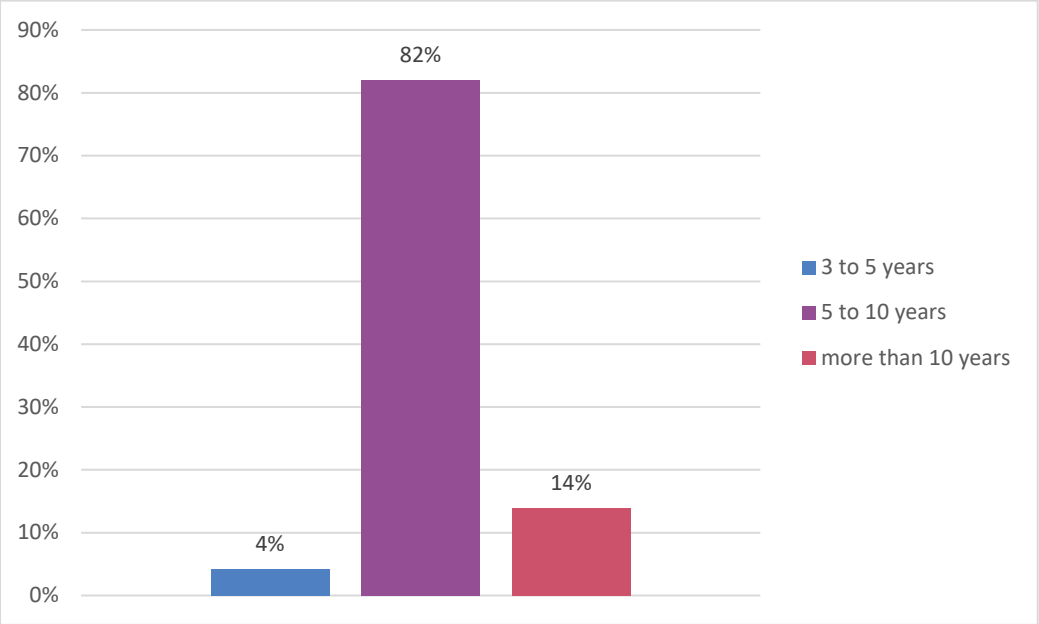

Figure 16 – 5G SA RAN equipment life cycle.

As presented in the graph, an overwhelming percentage of the operators that answered this question (82%) expect 5G RAN equipment to operate effectively for 5 to 10 years.

Question 32 - What strategy do you follow when replacing equipment?

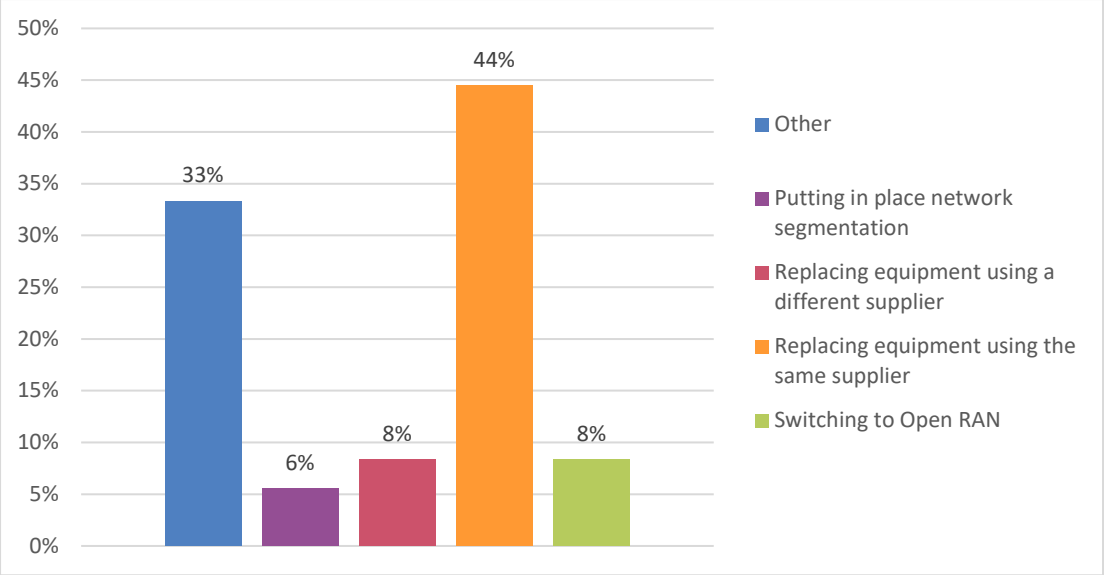

Figure 17 – Equipment replacement strategy.

44% of operators stated that they will follow a replacement strategy keeping the current vendor. A third of operators (33%) stated to follow a different strategy not mentioned in the options provided above. Amongst those following a different strategy or not naming a specific strategy, most stated that the evaluation process is not finalised yet and their strategy will depend on the results of ongoing technological and economic evaluations. Furthermore, it was stated that the strategy is multi-dimensional taking into account vendor lifetime recommendation, targeted use cases, capacity trends as well as hardware and software considerations (including vendor SLA and security factors). Others stated that the strategy regarding equipment replacement is defined by the group and is not in the decision-making authority of the regional branch.

The majority of operators intend to keep 5G non-SA mobile technologies (4G/5G hybrid) in service for more than 5 years. The expected life cycle of 5G SA equipment in Core network and 5G RAN components is 5-10 years. The equipment replacing strategy for 44% of the operators is keeping the current vendor. Others follow a range of different strategies like putting in place network segmentation replacing equipment using a different vendor, switching to Open RAN or will follow a different approach.

4 Findings

A number of findings can be clearly derived from the responses obtained, namely:

- 5G rollout is in its early phase, especially 5G SA and slicing.
- The majority of operators expect 5G non-SA Core to be in service for more than 5 more years.
- 5G SA equipment in the Core and 5G RAN is expected to operate effectively between 5 to 10 years.

- The majority of operators are of the opinion that the current standards (e.g. 3GPP/ETSI, ISO, GSMA) and guidance (e.g. ENISA) available for dual-core security are comprehensive and adequate.
- In the cloud based 5G SA core, the Access and Mobility Function (AMF) is considered as the network function with the highest level of risk.
- The vast majority of EU operators use cloud based services located within the EU. For cloud based architecture the majority of operators use their own private cloud.
- Multivendor strategy is progressing. Almost half of the operators that currently operate or plan to operate a 5G network use more than one vendor of 5G Core equipment and many of them have not encountered significant interoperability issues.
- Network Function Virtualization is widely used.
- The highest security risk factor identified is Isolation of Virtual Network Functions (VNF), followed by Administrator account compromise, the Compromise of Hypervisor, the Compromise of MANO, the Compromise of Host Kernel as well as the Multi-tenant virtualisation.
- The majority of operators did not need to change their plans regarding equipment vendor due to any decision related to the 5G Toolbox. However a significant minority had done this or are expecting to do so in the future.
- The majority of the operators responded that there is no framework in place on the substitution cost.
- Almost half of the operators stated that they will follow a replacement strategy keeping the current vendor.

5 Open Issues

How can we foster the multi-vendor strategy implementation in EU market?

What can we do to promote performing of the interoperability test for better resilience of the networks?

What measures can we put in place to support mitigation of the risk identified in cloud based 5G Core and virtualised networks?

Do we need to address lack of progress of the 5G SA deployment?

The equipment replacement costs have not been sufficiently analysed yet.

Annexes

Annex 1 – Questionnaires

NRA questionnaire:

	Technological challenges
1	Do you believe that it is necessary to **further** strengthen the role of national authorities with the adoption of strategic and/or technical measures and/or supporting actions?
2	If **Yes**, Please provide some details
3	If **Yes**, to 1, should this include additional regulatory powers for national authorities, to be able to use more effective ex-ante powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment?
4	If **Yes**, Please provide some details
5	Do you have in place any specific security legislative requirements on the CPE or other end user's devices?
6	Has your Country established a national IXPs strategy in order to promote the resilience of the internet infrastructure?
7	If **Yes**, Please provide some details
8	Under which framework are the IXPs currently regulated in your Country?
9	Please provide some details about the national legislation (e.g. links).
10	Are you currently the competent authority for IXPs?
11	If **No**, is it the NIS authority?
12	How many IXPs are there in your Country?
13	How many networks are connected to each IXP?

	Dependencies on other infrastructures
1	Is there any legal obligation for operators regarding emergency power supply in mobile networks in your country?
2	If **Yes**, is the obligation for the Core network?
3	If **Yes**, is the obligation for the Access network?
4	Is there any legal obligation in your country on how long Operators need to provide mobile services (e.g. emergency calls, SMS, telephony, internet) during a power outage?
5	Is there some fuel within the Country's commodity reserves planned to be delivered to the telecom operators in case of longer electricity outages (electricity reductions)?
6	Are there any guidelines for electronic communication service users to inform them about solutions (offered by operators) to avoid the customer's dependency on a single connection or provider?
7	If **Yes**, please provide additional information including any relevant links.
8	Is there any legislative requirement for having a national roaming in place for the case of an emergency situation?
9	Are you regulating subsea (submarine) cables?

	Dependencies on other infrastructures
10	If **yes** to the previous question, are there any specific security legal requirements for subsea cables?
11	If **yes** to question 9, do you have an overview of existing subsea cables?
12	Where to? In your territorial waters?
13	Where to? In your Exclusive Economic Zone?
14	Do you have an overview of planned subsea cables?
15	Where to? In your territorial waters?
16	Where to? In your Exclusive Economic Zone?
17	Do you have the information about the individual subsea cables?
18	Information such as: landing points?
19	Information such as: length?
20	Information such as: age?
21	Information such as: Ownership?
22	Information such as: Capacity?
23	Is the national subsea cables redundancy structure documented?
24	Do you have a crisis management plan for the disruption of subsea cables?
25	Are subsea cables critical infrastructure according to national CI definitions?

Operator questionnaire:

	Technological challenges on security
1	Do you support the following technologies in your network:
1a	Do you support 2G?
1b	Do you support 3G?
1c	Do you support 4G?
1d	Do you support 5G (4G core)?
1e	Do you support 5G Stand Alone (SA)?
2	If you support 5G what percentage is Stand alone?
3	If your network has a cloud based 5G SA core, which network function has the highest level of security risk?
4	Where are those cloud based functions located?
5	When you put in place mitigation measures against the identified risks to the Network Functions listed for the cloud based 5G SA core, do you follow standards and guidance from?
5a	ISO or other standards
5b	ENISA,
5c	3GPP/ETSI
5d	GSMA
5e	Other international standards
5f	National guidelines
6	Please provide details on those used.
7	For how long do you expect that 5G core will co-exist with 4G Core?
8	In your view, are there additional risks related to dual core (4G/5G)?

	Technological challenges on security
9	Did you need to take additional security measures when implementing dual core (4G/5G)?
10	Is there a need for additional standards or guidance related to the issue of security of dual 4G/5G core?
11	How many suppliers of 5G Core equipment (e.g. AMF, NEF, SMF) are you using?
13	How many of those vendors in the previous question are headquarter-based in:
13a	EU
13b	USA
13c	China
13d	South Korea
13e	Japan
13f	Other, please specify in comments column
14	Did you need to change your plans for equipment vendors due to any decisions at the national level based on the legislative requirements arising from the 5G Toolbox?
15	Is there a framework in place that regulates the substitution cost that you can rely on in case you would need to replace your equipment before its expected life cycle expires?
16	If **Yes**, please provide additional information including any relevant links.
17	Have you performed some interoperability testing for the equipment from different vendors?
18	Have you found any interoperability issues that you consider significant enough to prevent or limit their deployment in your network?
19	Do you use Network Function Virtualization in your core network?
20	If **Yes** to 19, what are the main security risk factors that you identified?
20a	Isolation of Virtual Network Functions
20b	Compromise of Host Kernel
20c	Compromise of Hypervisor
20d	Compromise of MANO
20e	Multi-tenant virtualization
20f	Administrator account compromise
20g	Other. Please specific in comments column
21	Have you identified any risks related to the network slicing?
22	Do you see regulatory demands as a limitation to deploy your infrastructure, according to best-practice IT- and cloud models?
23	If **Yes** to 22, please provide a brief description.
24	Do you see the need for any new legislative requirements on certain aspects of 5G networks security?
25	If **Yes**, would it be due to the need for harmonising the legislation in EU?
26	In deploying 5G SA, in your view, are there security benefits in utilizing virtualization and cloud services?
27	Please provide some details
28	With regard to your cloud-based architecture current or planned, will you use:

	Technological challenges on security
29	Concerning the customer equipment (e.g. CPE), what specific security measures do you have in place? Please specify.
30	Concerning smishing and vishing attacks, which exploit the lack of authentication and encryption in voice and SMS traffic, what specific measures do you have in place?
31	What mechanisms do you use in order to mitigate large-scale DDoS attacks?
32	Do you expect some help, support or explanations from NRA or other relevant EU institutions regarding NIS2 directive and its implementation and adjustments into your internal Cybersecurity processes?
33	Please provide some details
34	How much of your international traffic goes through the national IXPs? (percentage %)

	Equipment replacement
1	How much longer do you expect to keep 5G non standalone mobile technologies (4G/5G hybrid) in service?
2	What is the expected life cycle of 5G SA equipment in your core network?
3	What is the expected life cycle of 5G equipment for the RAN components in your network?
4	What strategy do you follow when replacing equipment?

	Dependencies on other infrastructures
1	What percentage of your network is equipped with permanent emergency power equipment (e.g. standby generators, batteries) in the **Core** network? %
2	What percentage of your network is equipped with permanent emergency power equipment (e.g. standby generators, batteries) in the **Access** network? %
3	What is the duration of the emergency power supply (batteries) for your network?
4	In order to cope with an energy emergency or outage can you implement technical measures e.g. disable particular **technologies** (2G, 3G) to reduce energy consumption?
5	In order to cope with an energy emergency can you implement technical measures e.g. disable particular **frequencies** to reduce energy consumption?
6	Does your company have access to mobile emergency power equipment (e.g. mobile generators)?
7	If **Yes, please specify**:
8	Do you have access to mobile base stations that can be distributed to disaster regions if needed?
9	If **Yes, please specify**:
10	Does your company use renewable energy (e.g. solar, wind) on mobile sites?
	If **Yes**
11	Is it **Standalone** (in combination with batteries)?
12	Is it in addition to regular power supply?
13	What kind of standby equipment as renewable energy source do you use for your base stations? At which percentage is used?

	Dependencies on other infrastructures
13a	Wind
13b	Solar
13c	Water
13d	None
14	Do you offer solutions to your customers to avoid the customer's dependency on a **single connection?**
15	Do you offer solutions to your customers to avoid the customer's dependency on a **single provider?**
16	Do you have in place any kind of roaming agreement with other national operators for the case of emergency situation?
17	Do you own any subsea (submarine) cables?
18	Are you using the subsea cables as a:
18a	Back up connection
18b	Primary connection
18c	Not using them
19	Do you use a direct interconnection with an external subsea cable provider?
19a	If **Yes**, as a Back up connection
19b	If **Yes**, as a Primary connection
20	If **Yes,** to the previous question (19), is the subsea cable provider with which you interconnect:
20a	Another Operator
20b	A dedicated subsea cable provider
20c	An OTT Provider
21	How do you ensure resilience with regards to your international connections over subsea cables?
22	Have you increased security or introduced any new security measures since last year in the contract with the subsea cable provider?
23	Do you use satellite communication networks for operating your services?
24	If **Yes** to the previous question, what services do you use satellite communication networks for:
	a. Back up connectivity only
	b. Universal service
	c. Voice services
	d. Internet access
	e. Emergency calls,
	f. M2M or IoT applications,
	g. TV broadcasting,
	other
25	What are the main cybersecurity challenges for these satellite networks?
26	Are you aware of recent incidents?
27	Please name them.

Annex 2 – National Regulatory Authorities participating in survey

NRA	**Member State/ Associated Country**
ACM	NETHERLANDS
AGCOM	ITALY
AKOS	SLOVENIA
ANACOM	PORTUGAL
ANCOM	ROMANIA
ARCEP	FRANCE
BIPT	BELGIUM
BNETZA	GERMANY
BTK	TURKEY
CNMC	SPAIN
ComReg	IRELAND
CRC	BULGARIA
CTU	CZECH REPUBLIC
DBA	DENMARK
ECOI	ICELAND
EETT	GREECE
EKIP	MONTENEGRO
ECPTRA	ESTONIA
HAKOM	CROATIA
ILR	LUXEMBOURG
MCA	MALTA
NMHH	HUNGARY
OCECPR	CYPRUS
PTS	SWEDEN
RAK	BOSNIA HERZEGOVINA
RATEL	SERBIA
RTR	AUSTRIA
RU	SLOVAK REPUBLIC
TRAFICOM	FINLAND
UKE	POLAND

Annex 3 – Member States and Associated Countries of participating operators

Member State/ Associated Country	**Number of operators**
BELGIUM	3
BOSNIA & HERZEGOVINA	14
BULGARIA	3
CROATIA	3
CYPRUS	4
CZECHIA	2
FINLAND	2
FRANCE	3
GERMANY	26
GREECE	4
HUNGARY	5
ICELAND	2
IRELAND	3
ITALY	8
LUXEMBOURG	3
MALTA	3
MONTENEGRO	4
POLAND	3
PORTUGAL	3
ROMANIA	7
SERBIA	3
SLOVAKIA	5
SLOVENIA	3
SPAIN	4
TURKEY	3
	123