BEREC
Body of European Regulators for Electronic Communications

BoR (23) 213

BEREC Report on the Current Cybersecurity Challenges and Dependencies in Electronic Communication Networks

7 December 2023

Contents

1 Executive summary 2

2 Introduction 2

3 Results 5

3.1 Dependencies on other infrastructures - Questionnaire for the NRA. 5

3.1.1 Emergency power supply obligations 5
3.1.2 Subsea cables 7

3.2 Technological Challenges - Questionnaire for the NRA. 9

3.1 **Error! Bookmark not defined.**

3.2.1 Internet Exchange Points 9
3.2.2 Customer Premises Equipment 11

3.3 Dependencies on other infrastructures - Questionnaire for the Operators 11

3.3.1 Subsea cables 17
3.3.2 Satellite networks 21

3.4 Technological Challenges for Operators 22

3.4.1 Customer equipment and other security measures 22
3.4.2 Mechanisms to mitigate large-scale DDoS attacks 23
3.4.3 NIS2 Directive and its implementation 23
3.4.4 International traffic through the national IXPs 24

4 Conclusions 26

4.1 Findings 29
4.2 Open issues and possible future work 31

5 Annexes 32

Annex 1 — Questionnaires 32

NRA questionnaire: 32
Operator questionnaire: 33

Annex 2 – National Regulatory Authorities participating in survey 36
Annex 3 – Member States and Associated Countries of participating operators 37
Annex 4 – Links to National Legislation 39
Annex 5 – List of figures 40

1 Executive summary

In 2023, the BEREC Cybersecurity Working Group conducted a comprehensive survey across European markets with the aim of gaining insights into the current state of resilience and cybersecurity in electronic communications networks. This survey, carried out through questionnaires, targeted both National Regulatory Authorities (NRAs) and operators, both fixed and mobile. It is the second iteration of such an effort, building upon the findings presented in BEREC's report on Secure 5G Networks.

The survey revealed various significant findings. From the NRAs' perspective, it explored issues such as dependencies on other infrastructures, specifically focusing on the legal and regulatory aspects of emergency power supply equipment in mobile networks across European countries. The results indicated varying degrees of national regulations in this regard, with cybersecurity frameworks often serving as a basis. The backup times for emergency power supplies and guidelines for informing users about reducing dependence on a single connection or provider during power outages were also investigated. Moreover, the survey inquired about national strategies for Internet Exchange Points (IXPs) aimed at enhancing internet infrastructure resilience.

From the operators' perspective, the survey delved into their views on emergency power supply equipment and network resilience. The majority of operators indicated comprehensive coverage of their core networks with permanent emergency power equipment. Backup times, strategies for reducing energy consumption during emergencies, and the use of renewable energy sources were among the subjects examined. Furthermore, it investigated customer dependency on a single connection or provider and roaming agreements. Subsea cables and satellite communication networks were also part of the survey.

Lastly, the survey explored the expectations of operators from National Regulatory Authorities (NRAs) and other EU institutions regarding the implementation and integration of the NIS-2 Directive into internal cybersecurity processes. They wish to ensure that the NIS-2 is transposed coherently and consistently through EU. It highlighted both positive and negative expectations, with many operators anticipating guidance, training, and collaborative efforts to effectively implement the NIS-2 Directive. The data gathered on the utilization of national Internet Exchange Points (IXPs) for international traffic revealed diverse approaches adopted by operators.

Overall, this survey presented valuable insights, further developed below, into the state of cybersecurity and resilience in European electronic communications networks, indicating areas for further additional investigation and potential improvements.

2 Introduction

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 mainly related to the dependencies on other infrastructures and some technological challenges for operators. The rest of the data gathered by this extensive questionnaire has already been presented in the BEREC's report on Secure 5G Networks[1]. The answers were gathered from the operators by the national independent regulators (NRAs) on a voluntary basis. Some questions were not applicable to all operators because they depend on the services offered. This generally explains why the number of respondents vary for each question. The total number of the answers gathered is presented in the analysis of each question.

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 14 April to 23 May 2023, with some individual extensions until 14 June. Answers from operators were collated nationally and were anonymised by the respective NRAs before they these were sent to BEREC. As a result, BEREC collected 123 answers from operators and 30 from BEREC members (NRAs) that were all provided on a voluntary basis. 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.

Questionnaire for the NRA:	
Technological Challenges:	Dependencies on other infrastructures:
Questions in scope of this report: 5 - 13	Questions in scope of this report: 1 - 25
Questions that were analysed in the first report: 1 - 4	Questions that were analysed in the first report: -

[1] BEREC Report Secure 5G networks (BoR (23) 180):
https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-secure-5g-networks

Questionnaire for the Operators		
Technological Challenges:	Equipment Replacement:	Dependencies on other infrastructures:
In scope of this report: 29 - 34	In scope of this report: -	In scope of this report: 1 - 27
The questions that were analysed in the first report: 1 - 28	The questions that were analysed in the first report: 1 - 4	The questions that were analysed in the first report: -

3 Results

3.1 Dependencies on other infrastructures - Questionnaire for the NRA.

3.1.1 Emergency power supply obligations

Question 1.1 Is there any legal obligation for operators regarding emergency power supply in mobile networks in your country?

The utilisation of emergency power supplies is an important factor that contributes to the resilience in mobile networks. However emergency power supplies can also be a significant cost driver as well as having a significant environmental impact especially when using batteries as a backup option.

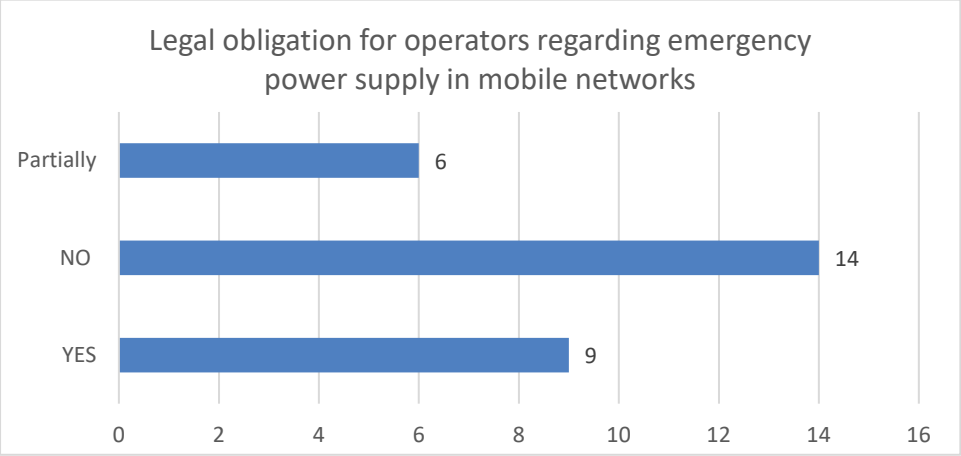

Figure 1 Is there any legal obligation for operators regarding emergency power supply in mobile networks in your country?

There were 29 answers to this question with 9 (31%) of NRAs having in place a specific national regulation on obligatory deployment of emergency power supply equipment in mobile networks. 6 (21%) of NRAs answered that they have partial regulation in force at the national level and 14 (48%) of the NRAs answered that there are no national obligations for the deployment of emergency power supply equipment in mobile networks.

Some additional explanations were provided by the NRAs. The legislation in place usually obliges the operators that carry out essential functions and services of the State and for such a purpose cybersecurity framework is used. A lot of additional comments provided by the NRAs mention the obligation of operators to adopt such measures that ensure the continuity of services during emergency situations according to the rules on the minimum security requirements of public electronic communication networks and services under the EECC framework.

Question 1.2 If Yes, is the obligation for the Core network?

Question 1.3 If Yes, is the obligation for the Access network?

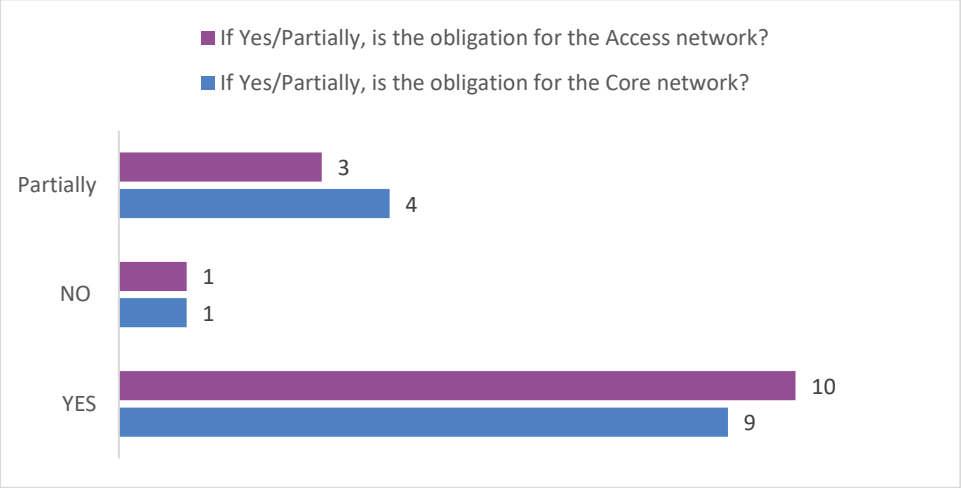

Figure 2 Legal obligation for the access network and/or core network

There were 14 responses to this question and 13 confirmed that their legal obligation regarding emergency power supplies was for the Core network.

13 NRAs confirmed the obligation for the Access network as well, out of those 3 NRAs imposed partial obligations on operators.

Question 1.4 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?

There were 30 answers to this question with 6 (20 %) NRAs confirming such legal obligation. Some additional explanations show that this obligation refers mostly to giving uninterrupted access to the emergency number 112 and in some cases for critical infrastructure. Where the back-up times of emergency power supplies were provided, they varied between 2 and 6 hours. In some countries, such obligations are not under the EECC but under the critical infrastructure framework.

Question 1.5 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)?

There were 26 answers to this question with 3 NRAs responding that there is some fuel reserved for telecom operators within the country's commodity reserves. In these cases, it is a national government decision or the matter of the national emergency supply agency to reserve and release the fuel supplies to the operators.

Question 1.6 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?
1.7. If yes, please provide additional information including any relevant links.

There were 28 answers to this question and all responded with a NO answer and therefore no further information was provided. Some NRAs did provide additional information on how they communicate the issue to the end users, such as when they suggest using a battery powered radio receiver or a car radio to ensure the reception of emergency warnings during power blackouts.

Question 1.8 Is there any legislative requirement for having a national roaming in place for the case of an emergency situation?

There were 27 answers to this question with 9 NRAs reporting mandating legislation for national roaming in emergency situations. In the vast majority of cases, this situation refers to the 112 calls that should be routed independently of the operator in case any network is down.

3.1.2 Subsea cables

Question 1.9 Are you regulating subsea (submarine) cables? Question 1.10 If yes to the previous question, are there any specific security legal requirements for subsea cables?

The 28 answers to the questions showed that half of the NRAs are regulating subsea cables. 2 of them confirmed that there are specific legal requirements on subsea cable security in their country.8 countries that have access to the sea do not regulate them.

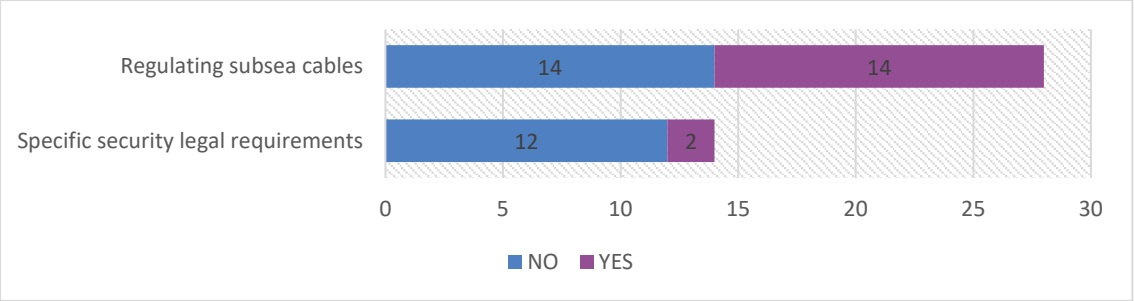

Figure 3 Regulation of subsea cables

Question 1.11 If yes to question 9, do you have an overview of existing subsea cables? Question 1.12 Where to? In your territorial waters? Question 1.13 Where to? In your Exclusive Economic Zone? Question 1.14 Do you have an overview of planned subsea cables? Question 1.15 Where to? In your territorial waters? Question 1.16 Where to? In your Exclusive Economic Zone?

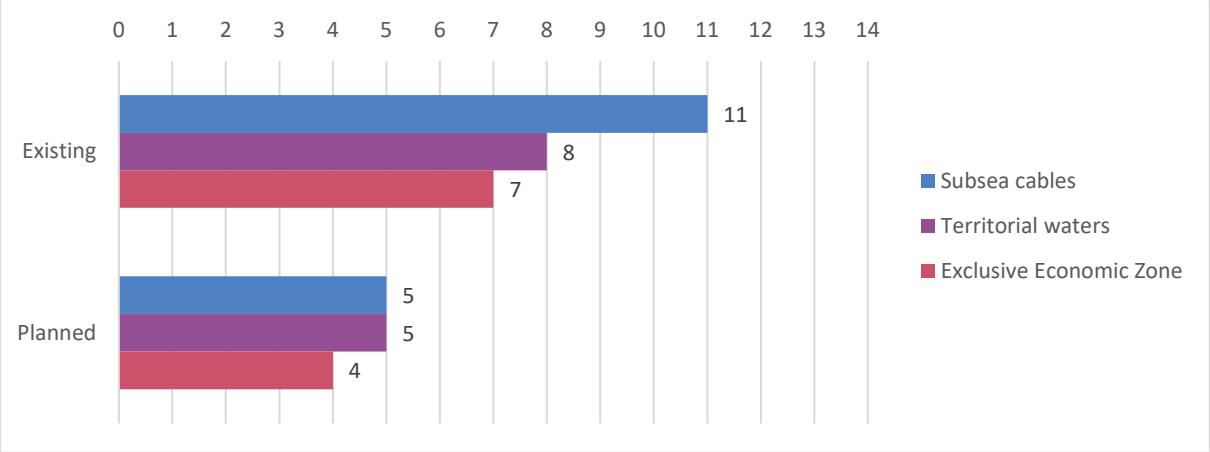

Figure 4 Location of existing and planned subsea cables

14 NRAs answered that they do regulate the subsea cables. These are broken down as follows[2]. 11 have an overview of the existing subsea cables. 8 of these for the existing subsea cables in the territorial waters and 7 to the Exclusive Economic Zone.

Of the 14 NRAs that answered that they do regulate the subsea cables, 11 have an overview of the existing subsea cables. 8 of these for the existing subsea cables in the territorial waters and 7 to the Exclusive Economic Zone.

5 of these 14 NRAs also have an overview of the planned subsea cables, 5 of these for the planned subsea cables to territorial waters and 7 out of these 14 to the Exclusive Economic Zone too.

Question 1.17 Do you have the information about the individual subsea cables?
Question 1.18 Information such as: Landing points?
Question 1.19 Information such as: Length?
Question 1.20 Information such as: Age?
Question 1.21 Information such as: Ownership?
Question 1.22 Information such as: Capacity?

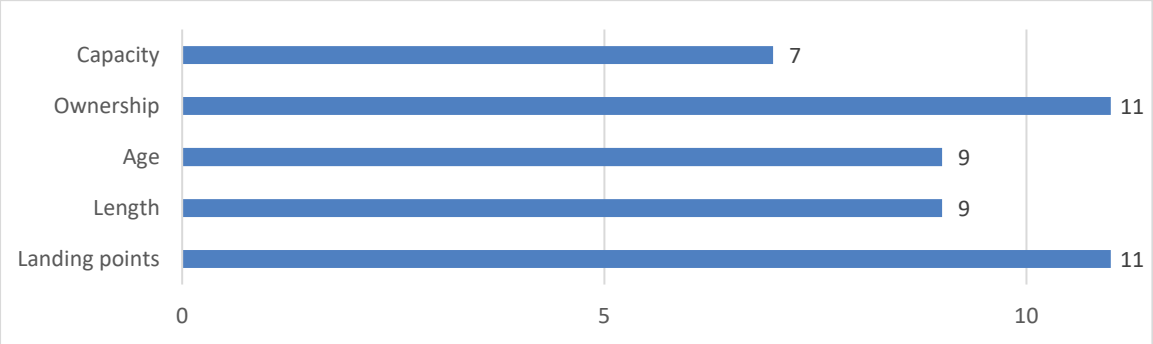

Figure 5 Type of information available on individual subsea cables

[2] note: some NRAs fall in multiple categories

29 answers were provided to this question. 11 NRAs have information about the individual subsea cables and 7 NRAs do not have this information. Of the 11 NRAs with this type of information, all have information on the ownership and landing points, 9 also on the age and length and 7 also on the capacity.

Question 1.23 Is the national subsea cables redundancy structure documented? Question 1.24 Do you have a crisis management plan for the disruption of subsea cables? Question 1.25 Are subsea cables critical infrastructure according to national CI definitions?

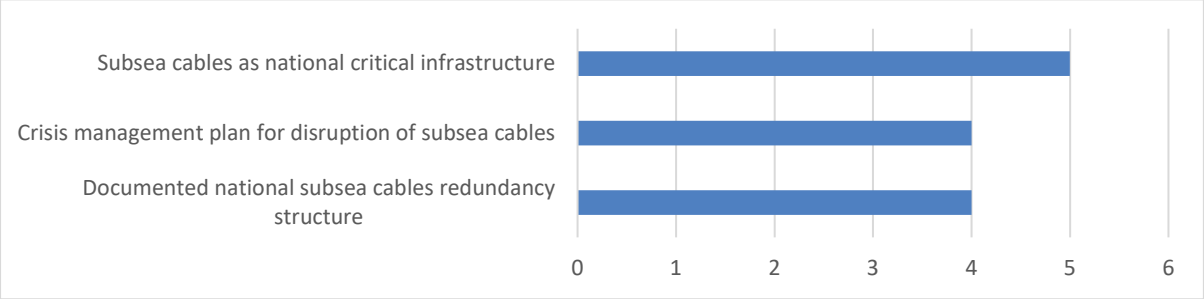

Figure 6 Documentation of subsea cables

Among the 16 NRAs that responded to question 1.23, 4 NRAs stated that the national subsea cable redundancy is documented.

Among the 17 NRAs that responded to question 1.24, 4 NRAs informed that they have a crisis management plan for the disruption of subsea cables.

Among the 16 NRAs that responded to question 1.25, 5 NRAs confirmed that subsea cables are considered as national critical infrastructure.

3.2 Technological Challenges - Questionnaire for the NRA.

3.2.1 Internet Exchange Points

Question 3.2.1 Has your Country established a national IXPs strategy in order to promote the resilience of the internet infrastructure? Question 3.2.2 If yes, please provide some details.

22 out of 25 NRAs responded that they do not have a specific national IXPs strategy in place in order to further promote the resilience of the internet infrastructure at a national level or such a strategy is not within the scope of their responsibility.

3 NRAs stated that they have a national IXPs strategy in place, with 2 of them stating that their national Cybersecurity strategy also includes the promotion of resilience of the IXPs within the borders of the Country.

Question 3.2.3 Under which framework are the IXPs currently regulated in your Country? Question 3.2.4 Please provide some details about the national legislation (e.g. links).

This question addresses the legal responsibility for regulating IXPs in the respective Country.

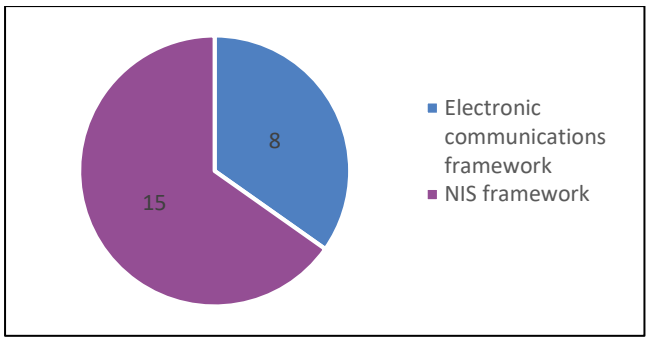

Figure 7 Framework regulating IXPs

The results of the survey showed that 15 (65%) of the NRAs answered that IXPs are currently regulated under the NIS framework in the respective countries, while 8 (35%) of the respondents stated that IXPs are currently regulated under the Electronic Communications framework.

15 NRAs provided additional information about the national legislation that is included in Annex 4 (Links to National Legislation) of this Report.

Question 3.2.5 Are you currently the competent authority for IXPs?
Question 3.2.6 If No, is it the NIS authority?

NRAs were asked to provide information on whether they are currently the competent authority for IXPs in their respective Country. The results showed that 16 out of 29 (65%) NRAs are the competent authority for regulating IXPs while 13 (35%) are not.

Where the NRA is not responsible for the regulation of IXPs, in most cases, another national authority assumes this responsibility.

Question 3.2.7 How many IXPs are there in your Country?
Question 3.2.8 How many networks are connected to each IXP?

This question aimed at getting an overview about the IXP infrastructure in the European Union asking for the number of IXPs in each country. The numbers stated only gave a rough indication as it correlates to the size of countries as well. The number of IXPs and the number of connected networks to the IXP reported by NRAs varied massively.

Still, the majority of the NRAs (16 out of 23) that provided the information stated to have 1 – 3 IXPs in their County. Other NRAs responded that they have 4, 6, 12, 15, 20 or 63 IXPs at national level.

As the size of IXPs reported under the question 3.2.7 varied across the countries, the number of connected networks also varied a lot. The numbers of networks connected to an IXP ranged from 2 to up to about 400.

3.2.2 Customer Premises Equipment

Question 3.2.9 Do you have in place any specific security legislative requirements on the CPE or other end user's devices?

27 NRAs responded to the question and 6 (22%) NRAs confirmed that they have security legislative requirements in their national legislations for CPEs or other end users' devices.

3.3 Dependencies on other infrastructures - Questionnaire for the Operators

Question 3.3.1 What percentage of your network is equipped with permanent emergency power equipment (e.g. standby generators, batteries) in the Core network?

91 out of 98 operators that answered this question stated that they have 100% of their core network equipped with permanent emergency power equipment while for the remaining 2 emergency power covers at least 90% of their core network. This robust adoption signified the paramount importance of maintaining uninterrupted power supply for core network operations. For the remaining 5 answers respondents the situation is the following: 2 operators have 70 - 80% of their core network covered with emergency power equipment and 3 have less than 35% covered. Out of the remaining operators one said that 100% of its core/aggregation/data center locations (ca. 1000) have emergency power and also have generators with backup-time for at least 48 hours. Another operator said that it has 60% of all sites equipped with generators or batteries, of which 48% are equipped with batteries only. A few sites do not have backup.

Question 3.3.2 What percentage of your network is equipped with permanent emergency power equipment (e.g. standby generators, batteries) in the Access network?

For this question 96 operators responded, of which 44 operators stated that they have 100% of their access network equipped with permanent emergency power equipment, and 20 operators have more than 90%. For some of the reasons also mentioned bellow, in the access network the coverage percentages are different. 13 operators answered that they have between 50% and 90% and 19 operators that have less than 50%.

Additionally, a small number of operators provided the reasoning of their choices for this question. One operator noted that only 2% of their mobile access network lacks backup but can be externally connected to mobile power generators. Another operator mentioned to have all sites equipped with batteries for its major sites that are representing approximately 10% of their network additionally with standby generators. Another operator revealed that roughly 25% of their its mobile access network lacks backup, while fixed fibre nodes have no backup at all as they are located on the customer premises. In contrast, aggregation nodes benefit from batteries and/or generators. One operator specified that only local HUBs are outfitted with standby generators and batteries, constituting a mere 5% of their network.

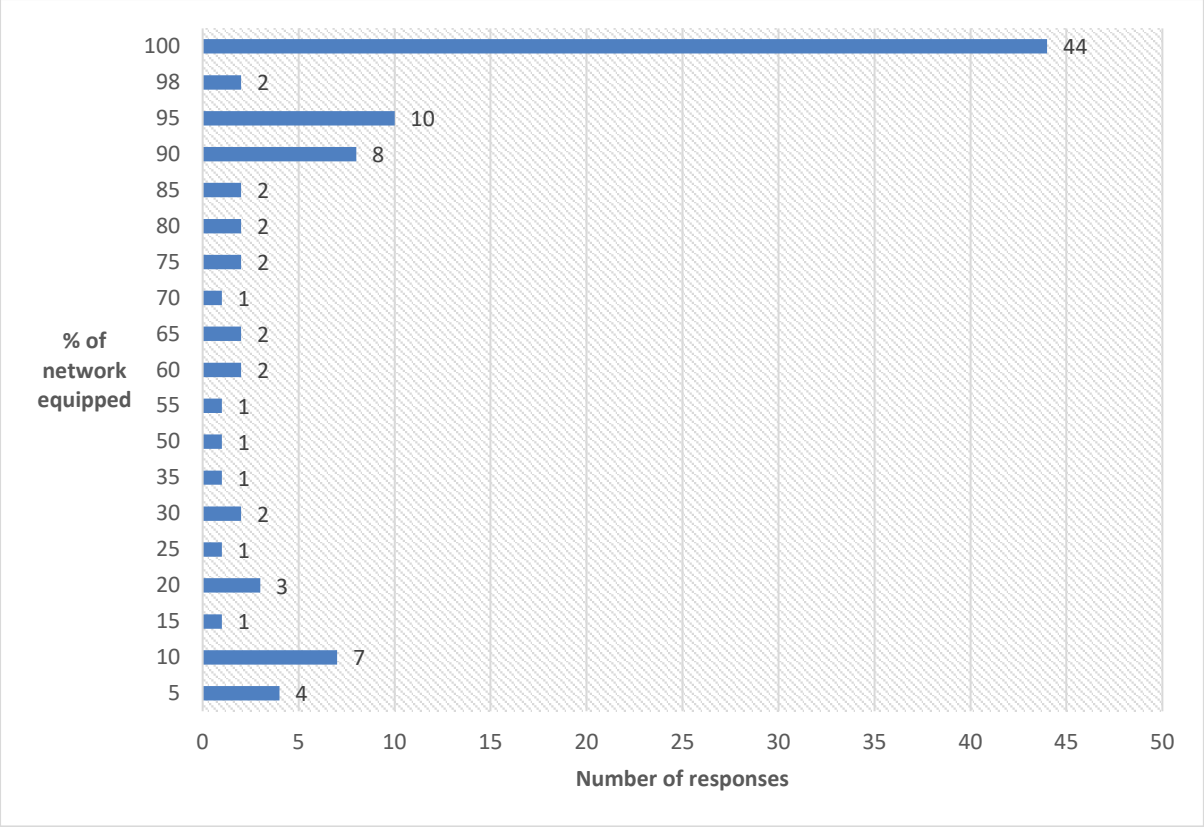

Figure 8 Permanent emergency power equipment in networks

Question 3.3.3 What is the duration of the emergency power supply (batteries) for your network?

Based on the answers of the operators regarding battery back up in both the core and access networks, operators were queried about the duration of their battery backups. From the 115 answers received, 12 operators were found to have limited battery backup, lasting less than 1 hour, 62 operators possessed medium battery capabilities, ranging between 1 and 3 hours and 41 respondents offered diverse time frames for their backup. Among the latter group, several operators provided examples and explanations. One operator said that in his country the legislation is under revision and there will be specific backup obligations for specific types of network equipment. Others specified that the backup lasts more than 4 or 6 hours, and others have different durations for Core and RAN backup. There are also operators that use different backup resources for central locations (up to 1 hour) and for locations less accessible (up to 6 hours). Other operators classify the assets/network equipment based on importance and allocate backup resources accordingly.

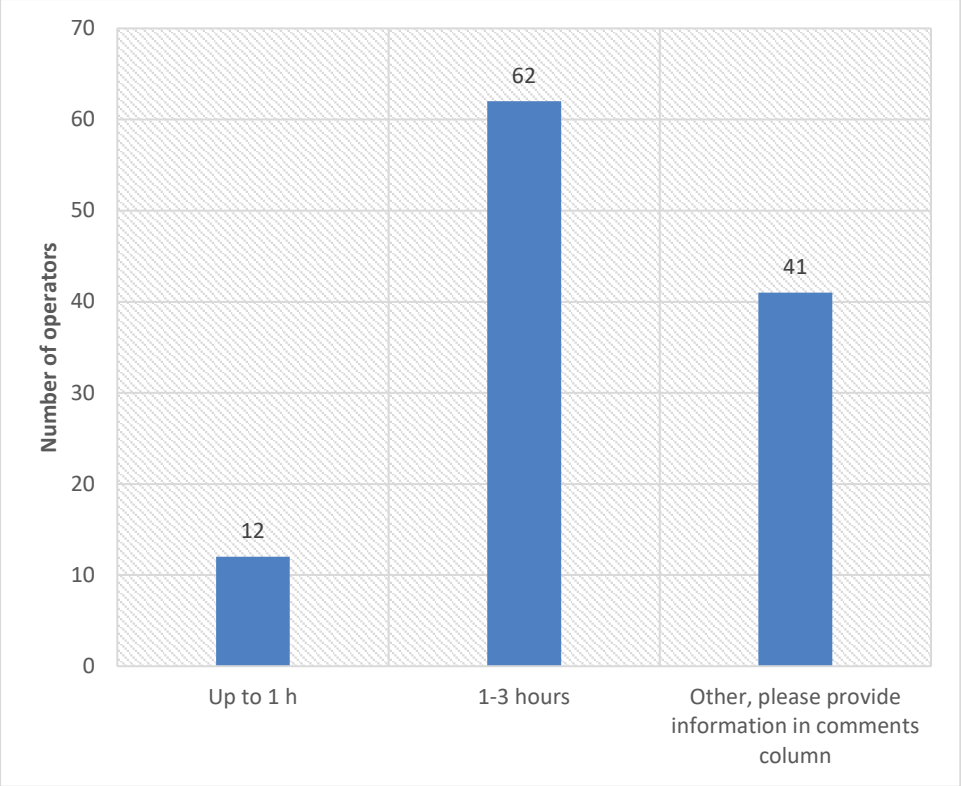

Figure 9 Duration of emergency power supply

Question 3.3.4 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?
Question 3.3.5 In order to cope with an energy emergency can you implement technical measures e.g. disable particular frequencies to reduce energy consumption?

This question aimed to test the stance of the operators about the prospects of reducing energy consumption during emergencies or outages by temporarily disabling specific technologies. The 108 operators responds to this question and are categorized as follows: 68 operators either have already taken steps or are considering implementing such measures, while 40 operators have not undertaken or contemplated such actions.

Several of the YES answers were accompanied by additional comments, such as: specific servers, data centres and network assets are disabled to save power. Migrating to more energy efficient platforms was mentioned as well and the dynamic switching off of higher frequencies (e.g. during the low consumption or while in a battery backup).

Some operators that provided NO answers claimed that such practices are not useful to reduce energy and stated that it cannot be done in the entire network and that it is depending on the network equipment type.

Operators provided some information on the possibility of deactivating specific frequencies (typically high frequencies or deactivate 4G) to achieve the energy-saving. They mention

dynamic saving energy features in off-peak times and depending on cell utilization motivated by economic reasons.

39 operators answered NO to the question about implementing technical measures e.g. disable particular frequencies to reduce energy consumption. They are concerned about potential drawbacks of such measures such as a service degradation and congestion.

Question 3.3.6 Does your company have access to mobile emergency power equipment (e.g. mobile generators)?
Question 3.3.7 If Yes, please specify:

There were 117 answers to the question 3.3.6. Based on these answers, 23 operators do not have access to mobile emergency power equipment, such as mobile generators. 94 (80%) operators responded YES to the question.

There were 72 answers to the question 3.3.7. Among operators with access to resources, various approaches were highlighted: some possess both in-house and external mobile generators, others exclusively rely on their own equipment, lacking access to external resources, and several have established Service Level Agreements (SLAs) with external suppliers for such equipment.

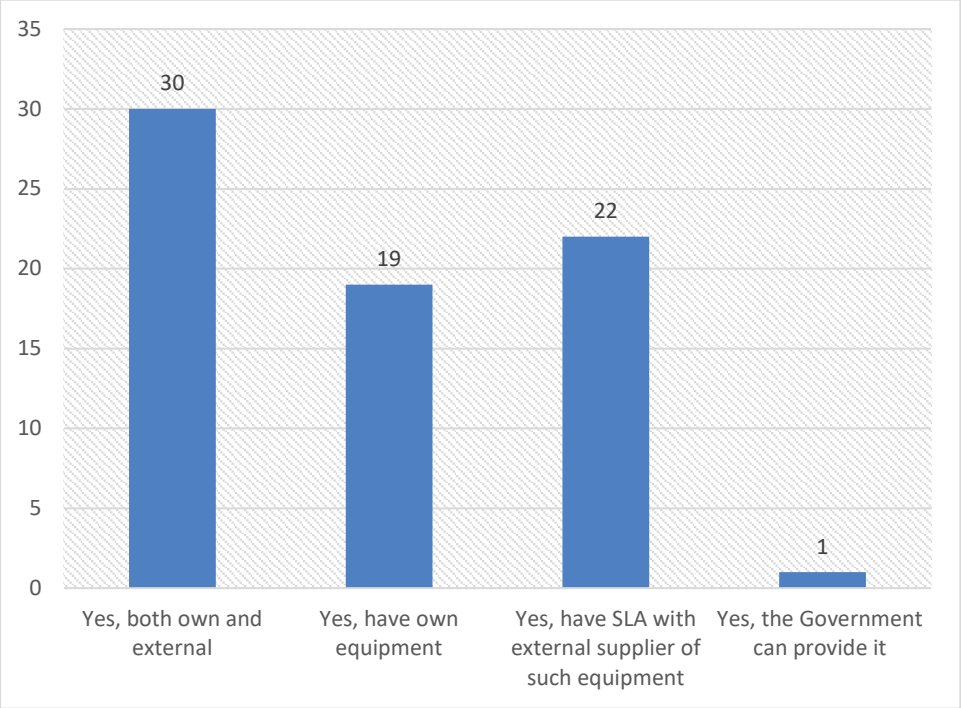

Figure 10 Access to mobile emergency power equipment

Question 3.3.8 Do you have access to mobile base stations that can be distributed to disaster regions if needed?

Operators were also queried about their access to mobile base stations that could be deployed to disaster-stricken regions when required. There were 106 answers to this question. The findings indicate that a significant majority, specifically 62%, possess this capability.

Question 3.3.9 If Yes, please specify:

There were 53 answers to this question. Among the operators with this capability some maintain both proprietary and external mobile base stations, others rely solely on their own base stations, lacking access to external resources. Several have established Service Level Agreements (SLAs) with external suppliers for such equipment.

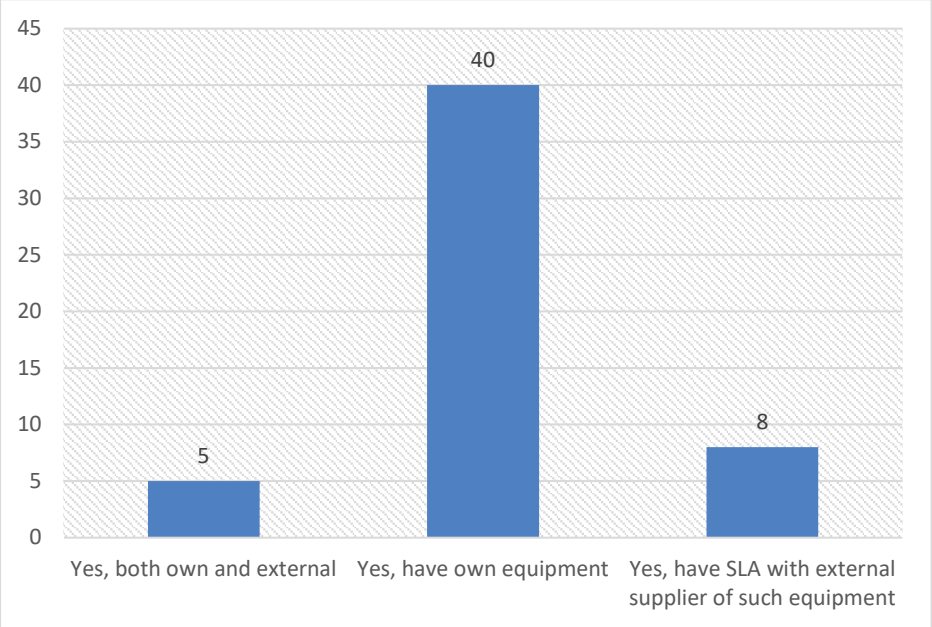

Figure 11 Access to mobile base stations for distribution to disaster regions

Question 3.3.10 Does your company use renewable energy (e.g. solar, wind) on mobile sites?
Question 3.3.11 If Yes to question 10, is it Standalone (in combination with batteries)?
Question 3.3.12 If Yes to question 10, is it in addition to regular power supply?

The survey aimed to explore diverse energy supply methods, including renewable sources. Among the 104 answers, 43 affirmed such utilization. Operators varied: some had their in-house systems, while others purchase renewable energy. One operator noted limited alternative energy at selected sites, while another claimed to be a 100% renewable energy user.

Upon further probing about the integration of renewable energy sources, the majority of the providers have a blended approach based on practical considerations where conventional sources are mixed with renewables.

Furthermore, operators were probed about integrating renewable energy. The majority adopted a flexible approach, blending renewables and conventional sources based on practical considerations.

Question 3.3.13 What kind of standby equipment as renewable energy source do you use for your base stations? At which percentage is used?

Question 3.3.13a Wind
Question 3.3.13b Solar
Question 3.3.13c Water
Question 3.3.13d None

The operators were requested to furnish additional details concerning the specific renewable energy sources employed to support normal and stand-by operations. It is worth noting, as a general observation, that the adoption and utilization of alternative energy sources appear to be in their nascent stages within this context.

Regarding the use of wind energy as an alternative source, only six operators indicated that approximately 1% of their network is powered by wind energy. Additionally, some of these operators deploy a combination of multiple renewable energy sources, including wind, solar, and hydroelectric power. However, it's noteworthy that even among these operators with a mix of energy sources, the individual percentages allocated to each source do not exceed 1% of their total energy generation capacity.

The solar energy systems are more widely adopted by operators, often at higher percentages than wind-based alternatives. The data reveals that a total of 12 operators have integrated solar energy sources into their networks, with reported utilization ranging between 1% and 10% of their total energy generation capacity. Additionally, a notable subset of 4 operators exceeds the 10% mark in their reliance on solar energy. Remarkably, in comparison to other alternative energy sources, solar systems exhibit a higher prevalence among operators, with a substantial 21 operators incorporating solar energy solutions into their infrastructure.

The least prevalent option among renewable energy sources appears to be water-based energy generation. Our data indicates that only a minimal number of operators, specifically three, incorporate water-based energy sources into their networks. Among these three operators, two allocate a modest 1% of their energy generation capacity to this source, while the third operator stands out with a considerably higher utilization rate, exceeding the 10% mark.

Question 3.3.14 Do you offer solutions to your customers to avoid the customer’s dependency on a single connection?
Question 3.3.15 Do you offer solutions to your customers to avoid the customer’s dependency on a single provider?
Question 3.3.16 Do you have in place any kind of roaming agreement with other national operators for the case of emergency situation?

There were 110 answers to question 3.3.14. Almost 75% of the providers that answered this question offer solutions to their customers to avoid the dependency on a single connection.

There were 106 answers to question 3.3.15. 40% of the providers (43 out of 106) that answered this question offer solutions to avoid the dependency on a single provider.

There were 106 answers to question 3.3.16. Less than 20% of providers have a roaming agreements in place with other national providers for emergency situations.

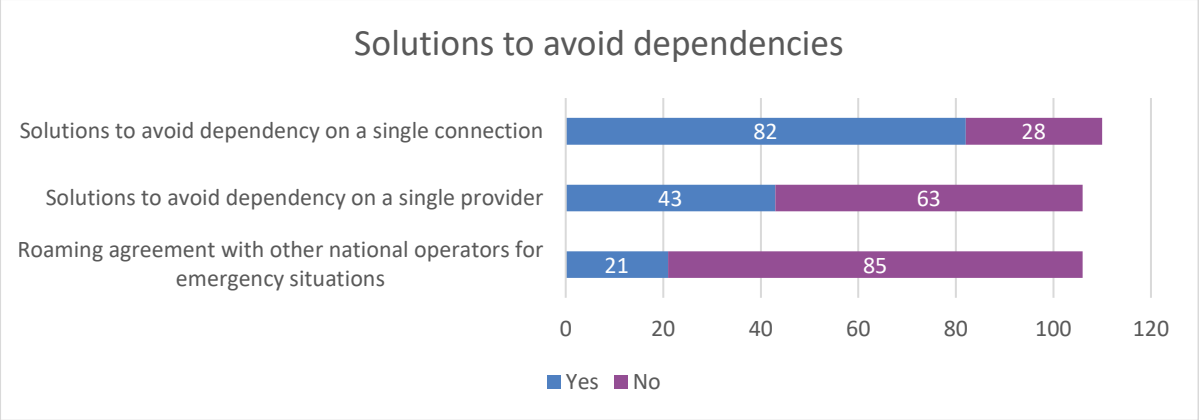

Figure 12 Solutions to avoid dependencies

3.3.1 Subsea cables

Question 3.3.17 Do you own any subsea (submarine) cables?

Out of the 105 answers received to this question, 84 (80%) of them stated “NO”, they do not own any subsea cables while 21 (20%) replied “YES”, they do own subsea cables.

Question 3.3.18a Are you using the subsea cables as a: Back-up connection

There were 62 answers to this question, 36 (58%) replied “NO”, they do not use subsea cables as a back-up connection while 26 (42%) said that they do use subsea cables as a back-up connection.

Question 3.3.18b Are you using the subsea cables as a: Primary connection

There were 61 answers to this question, 36 (59%) replied “YES”, they do not use subsea cables as a back-up connection while 25 (41%) said that they do use subsea cables as a back-up connection.

Question 3.318c Are you using the subsea cables as a: Not using them

The 57 answers stated that 32 (56%) replied “YES”, they use subsea cables while 25 (44%) said that they are not using them.

Question 3.3.19 Do you use a direct interconnection with an external subsea cable provider?

There were 95 answers to this question in which 65 (68%) do not use a direct interconnection with an external subsea cable provider and 30 (32%) answered “YES” they use a direct interconnection with an external subsea cable provider.

Question 3.3.19a If Yes, as a Back-up connection Question 3.3.19b If Yes, as a Primary connection

As a follow-up to Question 19 out of the 39 answers, 26 (67%) said “YES” they use their direct subsea cable interconnection as a back-up and 13 (33%) answered “NO”.

As a follow-up to Question 19, there were 38 answers to this question, 28 (74%) said “YES” they use their direct subsea cable interconnection as a Primary connection and 10 (26%) answered “NO”.

As a summary for Questions 19a and 19b, 28 operators use their direct interconnection with an external subsea cable provider as a Primary connection while 26 operators use it as a Back-up connection.

Question 3.3.20 If Yes, to the previous question 19 (use of a direct interconnection with an external subsea cable provider), is the subsea cable provider with which you interconnect:
a) Another Operator
b) A dedicated subsea cable provider
c) An OTT Provider

This question was a follow-up to question 2.19, it further explored the ownership of the external subsea cables used for direct interconnection by operators.

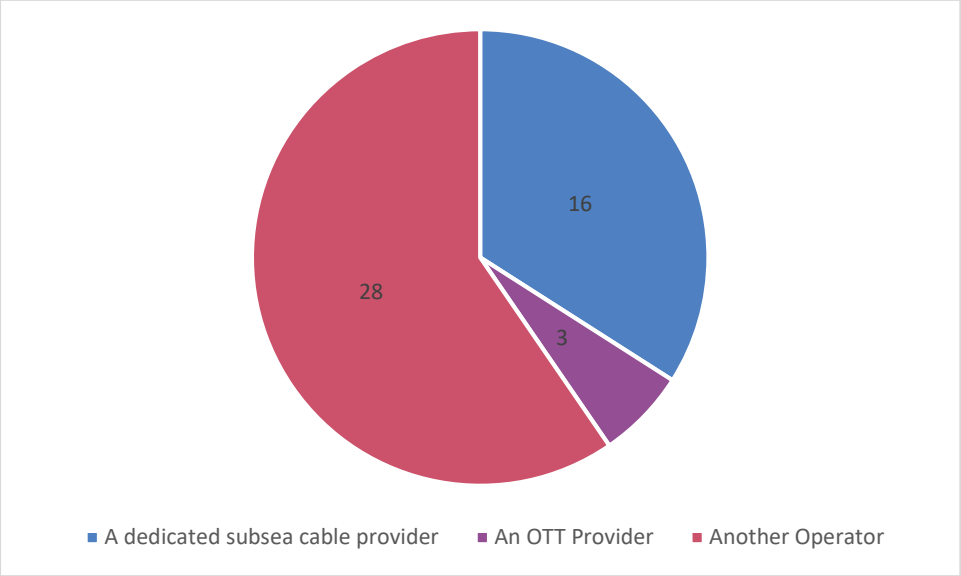

Figure 13 Ownership of externally provided subsea cables

Out of the 30 operators who replied in Question 19 that they have a direct interconnection with an external subsea cable provider, 28 said that the subsea cables were owned by another operator, 16 operators replied that they were owned by a dedicated subsea cable provider while 3 operators used cables owned by OTT providers. With a total of 47 external operators named, it is possible that some operators have more than one direct interconnection with an external subsea cable provider.

Question 3.3.21 How do you ensure resilience with regards to your international connections over subsea cables?

As illustrated in Figure 12, the majority of the answers (32 operators) that do use subsea cables for resilience use them as back up circuits.

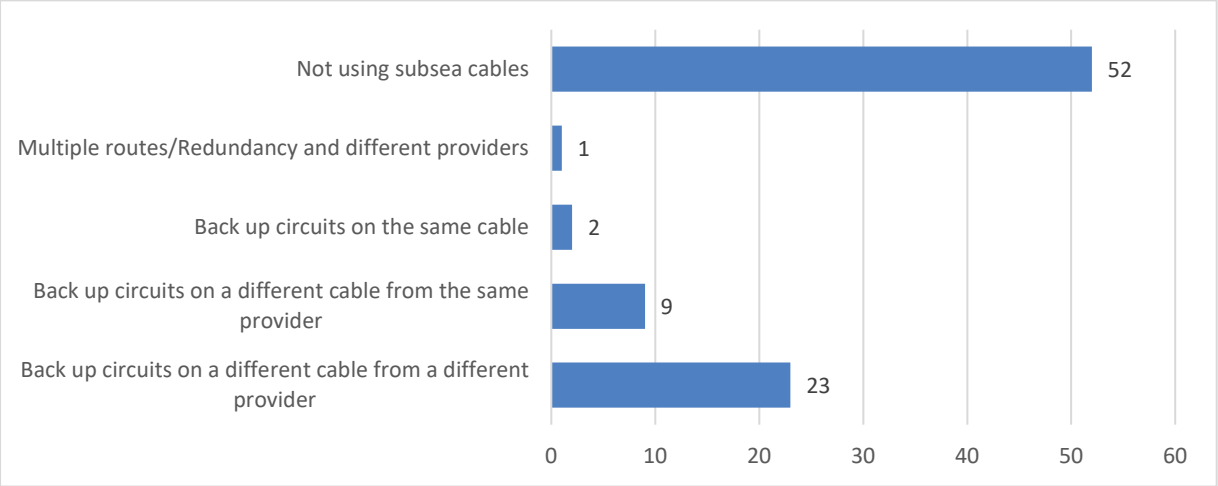

Figure 14 Methods to ensure resilience over subsea cable connections

Question 3.3.22 Have you increased security or introduced any new security measures since last year in the contract with the subsea cable provider?

There were 88 answers to this question. As illustrated in Figure 16, the majority of the answers (32 operators) that do use subsea cables have not increased security or introduced any new security measures since last year in the contract with the subsea cable provider.

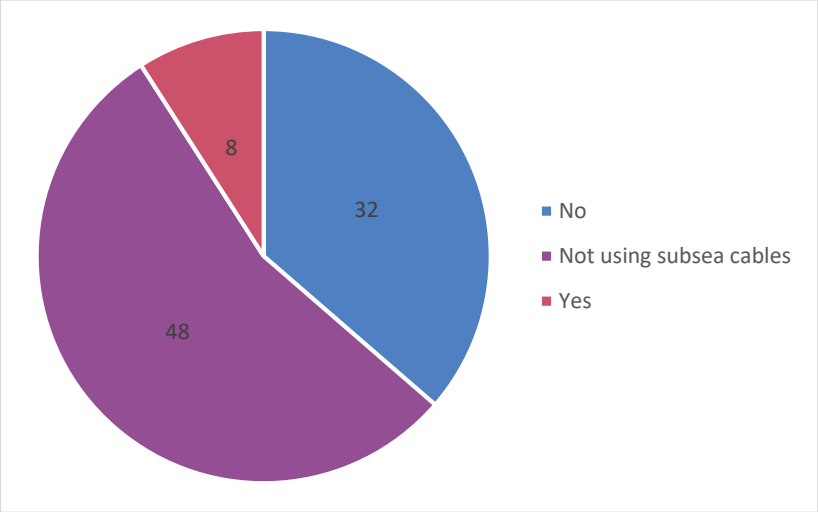

Figure 15 Increased security or introduction of new security measures since last year

Question 3.3.23 "Do you use satellite communication networks for operating your services?

From the 106 answers to this question, 66 (62%) operators answered that they do not use satellite communication networks for operating their services.

Question 3.3.24a If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: Back up connectivity only

As a follow-up to Question 3.3.23, there were 39 answers to this question, 11 operators use satellite communication networks for Back up connectivity only.

Question 3.3.24b If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: Universal service

As a follow-up to Question 3.3.23, there were 40 answers to this question, 7 operators you use satellite communication networks for Universal service.

Question 3.3.24c If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: Voice services

As a follow-up to Question 3.3.23, there were 40 answers to this question, 15 operators use satellite communication networks for Voice services.

Question 3.3.24d If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: Internet access

As a follow-up to Question 3.3.23, there were 41 answers to this question, 18 operators use satellite communication networks for Internet access.

Question 3.3.24e If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: Emergency calls

As a follow-up to Question 3.3.23, there were 41 answers to this question, 13 operators use satellite communication networks for Emergency calls.

Question 3.3.24f If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: M2M or IoT applications

As a follow-up to Question 3.3.23, there were 37 answers to this question, 7 operators use satellite communication networks for: M2M or IoT applications.

Question 3.3.24g If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: TV broadcasting

As a follow-up to Question 3.3.23, there were 41 answers to this question, 27 operators use satellite communication networks for TV broadcasting.

Question 3.3.24h If Yes to the previous question 3.3.23, what services do you use satellite communication networks for: other

As a follow-up to Question 3.3.23, there were 22 answers to this question, 13 operators use satellite communication networks for other means.

A summary of Questions 3.3.24a – 3.3.24h is illustrated in Figure 17. The main service that operators use for Satellite Communication Networks is TV Broadcasting, followed by Internet Access and then Voice Services.

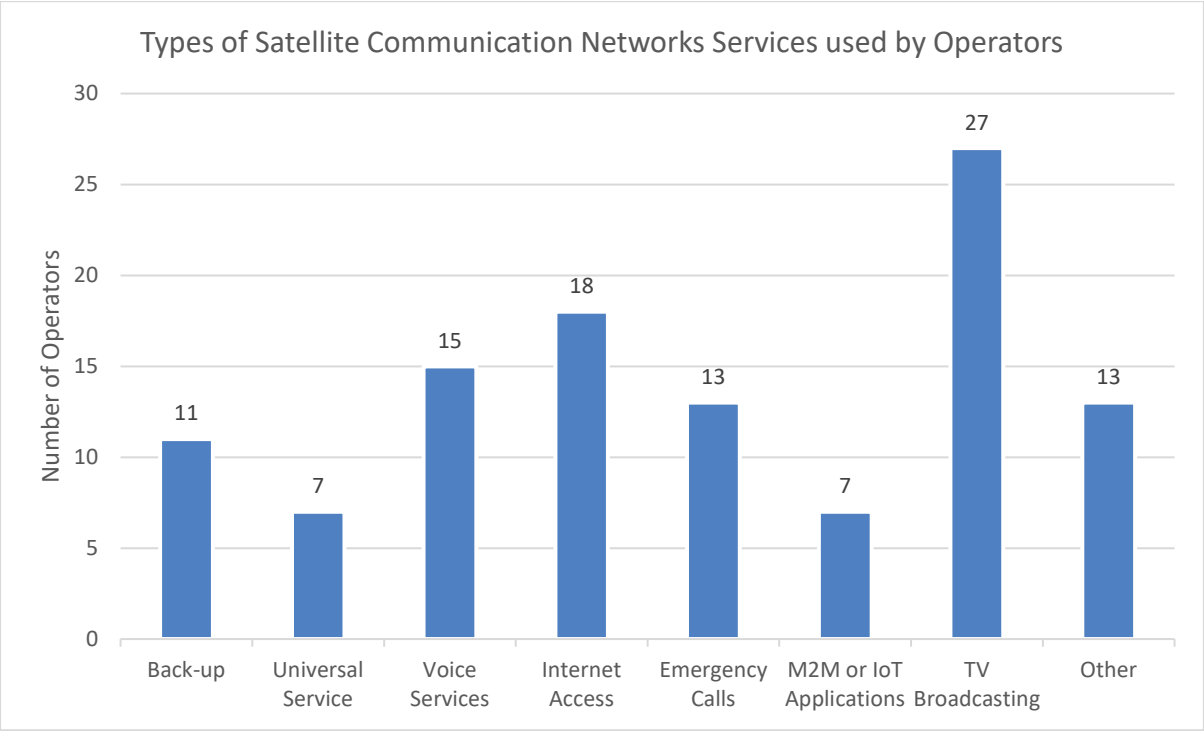

Figure 16 Types of Satellite Communication Networks Services

3.3.2 Satellite networks

Question 3.3.25 What are the main cybersecurity challenges for these satellite networks?

According to the answers received, operators identify a wide range of cybersecurity challenges, which we group into risks arising from the electronic, software-based and physical aspects of the network.

Electronic attacks that were repeatedly mentioned are jamming and spoofing, GPS/GNSS and signal interference, breaches of the confidentiality aspect of physical layer confidentiality (through the use of eavesdropping antennas) and compromising of the integrity of earth stations by using malicious messages, e.g. OTA (over-the-air) provisioning messages.

Software-based risks and challenges included, among others, user authentication issues, malware and hacking protection, a lack of standardised security protocols and lack of alignment of manufacturer's practices with the requirements of operators (as well as with the relevant standards without compromising the operation of the network).

Physical challenges, such as the prevention of physical breaches constitute an additional dimension of cybersecurity challenges. As well as the resistance and robustness of the supply chains.

In addition to the above, legal and regulatory challenges were also mentioned.

Question 3.3.26 Are you aware of recent incidents?
Question 3.3.27 If yes, in previous question 3.3.26, Please name them?

Out of the 68 operators' answers, 60 (88%) reported no awareness of recent incidents. However, those with knowledge of such incidents cited several examples.

Satellite jamming emerged as a recurring issue, with multiple major incidents noted in northern Europe, all associated with the Russian/Ukraine conflict. Additionally, operators mentioned the "Soft Cell" operation targeting Vodafone in Portugal (APT Gallium. Another incident involved a cyberattack on the Ka-Sat service, owned by Viasat, impacting a significant number of customers.

3.4 Technological Challenges for Operators

3.4.1 Customer equipment and other security measures

Questions 3.4.1 Concerning the customer equipment (e.g. CPE), what specific security measures do you have in place? Please specify.

Operators were asked on the security measures they have in place regarding their customer equipment. There were 53 answers to this question in which operators listed a multitude of measures that are used to address internal device security, external device security and network controlled device security. These included automatically configured firewalls, device hardening, patch management, bug fixing, penetration testing during the manufacturing (development) stage, isolation of traffic, encryption security protocol protection, managed authentication requirements for access and implementation of the endpoint-security solution. In addition, remote management through an ACS (Auto Configuration Service) to push new firmware for security vulnerabilities with encrypted communication between the CPE and ACS, deploy UPF (User Plane Function) at the EDGE with additional security rules, Remote Triggered Black Hole (RTBH) to block unwanted traffic from DDoS attacks, periodic staff training and continuous risk awareness/simulation campaigns.

Question 3.4.2 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?

Operators were asked on the specific measures they have in place concerning smishing and vishing attacks, which exploit the lack of authentication and encryption in voice and SMS traffic. 62 operators provided a short description of measures put in place.

Most of the operators have multiple measures in place regarding phishing and vishing. These include preventive, detective and reactive measures.

Preventive measures include trainings and raising awareness, which is important to identify scam calls and SMS's to be able to take the appropriate responses.

Blocking or filtering is a commonly used measure. They do this through blacklisting or firewalls and is often based on the CLI to prevent spoofing. These systems analyse traffic patterns, origin, sender, volume, and destination to identify and prevent potential threats. Voice and SMS spam firewalls, including AI-based solutions are used. Filtering at the signalling level (e.g. DIAMETER and SS7) is also used. Providers use commercial solutions but some also use internally developed protection tools.

Multiple providers refer to frameworks such as STIR/SHAKEN or national systems put in place to prevent the exploitation. Several providers mentioned the importance of cooperation, regulatory measures and suitable legislation that allows or requires to take measures to prevent smishing and vishing attacks.

Detective measures include monitoring of the traffic and customer complaints. Through detailed investigations by the SOC or fraud analysts of the provider can find out which reactive measures to take. Usually blocking will prevent future attacks but detection methods must improve.

The way the question was formulated does not allow the analysis of the number of operators using the different methods. Therefore, a more thorough investigation would be useful.

3.4.2 Mechanisms to mitigate large-scale DDoS attacks

Question 3.4.3 What mechanisms do you use in order to mitigate large-scale DDoS attacks?

Operators were asked about the mechanisms they use to mitigate large-scale DDoS attacks. There were 74 answers to this question. Only 5 operators answered they did not have any particular mechanisms to mitigate DDoS attacks. The answers provided by the operators show they are using various solutions provided by different suppliers at multiple layers. Among them, there are internal and external solutions for detecting, monitoring and mitigating large attacks. Measures mentioned include anti DDoS protection on multiple layers, administrative measures, routing modification, firewalls and port blocking, network segmentation/isolation and zoning, limiting the number of concurrent sessions, cloud-based scrubbing and blackhole routing as last resort.

Most of the operators use DDoS protection through internal and/ or external platforms.

3.4.3 NIS-2 Directive and its implementation

Questions 3.4.4 Do you expect some help, support or explanations from NRA or other relevant EU institutions regarding NIS-2 Directive and its implementation and adjustments into your internal Cybersecurity processes? Questions 3.4.5 Please provide some details.

Operators were asked whether they expect some help, support or explanations from the NRA or other relevant EU institutions regarding the NIS-2 and its implementation and adjustments

into the internal Cybersecurity processes. 67 operators responded to this question and the majority (37) provided a positive answer while 30 operators do not expect help on that matter.

Operators put forward that the electronic communications sector has recently undergone a significant effort to comply with national regulation on the security and integrity of electronic communications networks and services as a result of the transposition of the EECC directive, therefore they believe that it would be useful to have a thorough and comprehensive listing of the additional requirements posed by the NIS-2.

In the answers there was a common call to European Commission, BEREC, ENISA and national authorities (and legislators) to ensure that the NIS-2 is transposed coherently and consistently through EU. Implementing acts foreseen for adoption by the Commission in 2024 play an important role in achieving the objectives mentioned. Expectations about the support from the NRA (BEREC) and national Cyber Security authority on one side as well as ENISA and the Commission on the other side through clear recommendations, white papers and transparent regulation were mentioned. The topics mentioned were clear rules for the cybersecurity risk-management measures described in NIS-2 and problem of incident reporting to different authorities for same incidents. The issue of short timeframe and the risk of incorrect NIS-2 implementation by the companies on the national level was also stated.

Financial support, but without giving further details, was also mentioned and the need to take into account existing national cybersecurity legislation.

3.4.4 International traffic through the national IXPs

Question 3.4.6 How much of your international traffic goes through the national IXPs? (percentage %).

Operators were asked to indicate the percentage of traffic that goes through the national IXP's. There were 57 answers to this question.

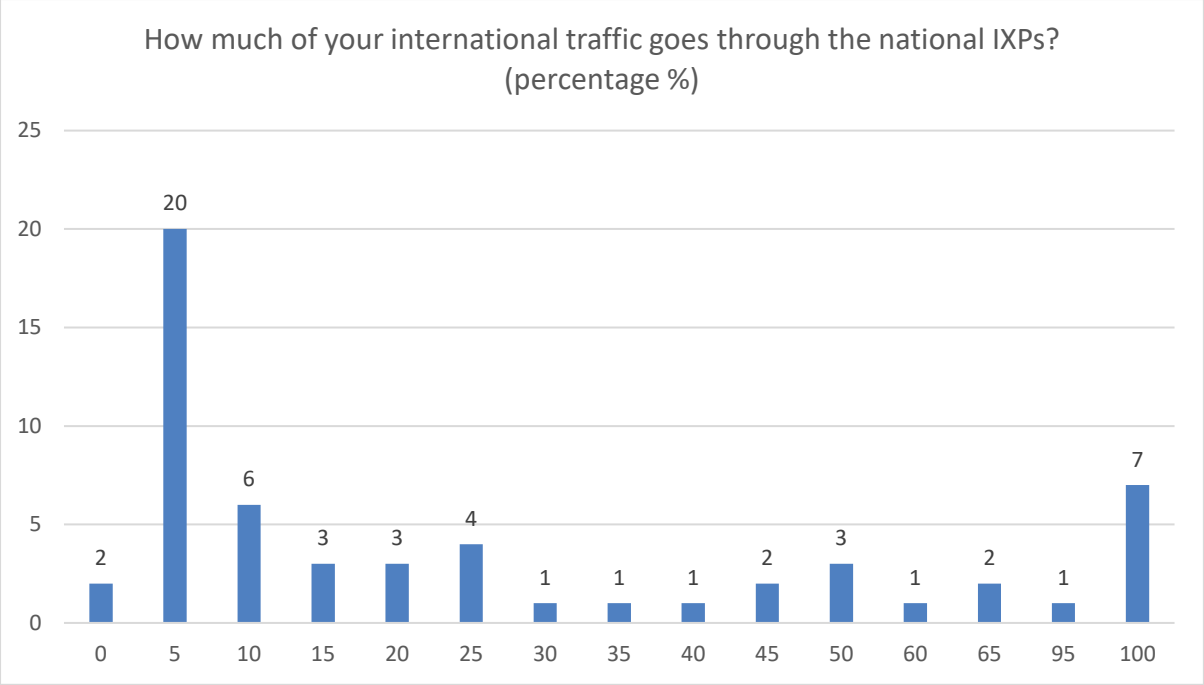

Figure 17 Percentage of international traffic going through national IXPs

Most of the respondents (20) answered that 5% of their traffic goes through the national IXPs. Second largest number of operators (7) answered that all their traffic pass through the national IXPs, while 2 operators don't send any international traffic through the national IXP.

2 operators noted that the national IXP is used for national traffic exchange. 1 operator clarified that international traffic is routed towards the internal backbone unless the national IX offers NPI (Network Peering interconnection) that is more convenient. Typical examples are OTT's or international backbone operators that have their own peering point in the national IXs.

Most of the operators have a small percentage of their international traffic going through the national IXP's.

4 Conclusions

A number of conclusions can be clearly derived from the answers obtained, namely:

- **Dependencies on other infrastructures, from NRAs perspective**

- The use of emergency power supplies is an important factor that contributes to reliability in mobile networks. However, emergency power supplies can also be a significant cost driver.

- Only a small number of countries have specific national regulations for emergency power supplies in mobile networks, some have partial regulations, while others reported no national obligations. Additional explanations revealed that such obligations often target operators providing essential state functions and services, with cybersecurity frameworks frequently serving as a basis. Many NRAs pointed to operators' responsibilities for ensuring service continuity during emergencies, aligning with the Rules on minimum security requirements for electronic communication networks and services under the EECC framework.

The backup times for emergency power supplies, where specified, ranged from 2 to 6 hours. Some countries indicated that these obligations fell outside the scope of the EECC framework, targeting critical infrastructure.

- In response to queries regarding the existence of guidelines for informing electronic communication service users about solutions to reduce dependence on a single connection or provider during power outages, all NRAs responded negatively. However, several NRAs provided additional insights into how they communicate with end users during such scenarios, often suggesting solutions like using battery-powered radios or car radios for receiving emergency warnings.

- National roaming, in emergency situations legislation exists in some countries, while in most cases, this legislation pertains to ensuring the independent routing of 112 emergency calls in the event of network disruptions. Due to many natural disasters reoccurring every year in Europe this topic could be further investigated.

- Nearly half of the NRAs reported that they regulate subsea cables, with most of these countries having specific legal requirements for enhancing security in this context. But also 8 countries that have access to the sea do not regulate them.

- **Technological Challenges, from NRAs perspective**

While the Internet is designed with a strong emphasis on resilience, this question focused on possible national strategies to further strengthen the internet infrastructure at a national level. The survey examined the presence of a national strategy for Internet Exchange Points (IXPs). Internet Exchange Points (IXPs) are seen as the main Internet switching centres as they provide the infrastructure for both public and private Internet peering.

The results revealed the following:

- The regulatory landscape is not very diverse, with around half of the NRAs indicating that IXPs are governed under the Network and Information Systems (NIS) framework, and approximately a third regulated within the Electronic Communications framework.

- The survey revealed a balanced distribution of NRAs being/not being in charge of regulating IXPs. In cases where NRAs did not regulate IXPs, the NIS authority often took up this responsibility.

- The number of IXPs in countries varied, with most NRAs reporting between 1 to 3 IXPs. However, there were some exceptions that included NRAs reporting higher counts, such as 12, approximately 20, or even 63 IXPs at a national level.

- The number of networks connected to IXPs ranged significantly due to variations in IXP sizes, from 2 to roughly 400 networks per IXP.

- **Dependencies on other infrastructures – from Operators perspective**

The survey results inquired about various aspects of emergency power supply equipment and network resilience within the telecommunications sector and were addressed directly to the operators. The findings are listed as follows:

- A vast majority confirmed that their entire core network is equipped with permanent emergency power equipment, emphasizing the significance of uninterrupted power for core network operations. On the other hand, half of the operators have all of their access networks fully covered, while the rest exhibit a varying level of coverage percentages.

- The backup times for emergency power supplies, where specified, ranged from 1 to 3 hours for more than half of the respondents, while the rest of the respondents have diverse time frames for their backup. Several operators explained their specific situations, including variations in backup times, revised legislation, and allocation based on asset importance.

- When asked about the ability to reduce energy consumption by disabling technologies during emergencies, part of the operators have already taken steps or are considering it. They have also shared comments on this, including the selective disabling of servers, network assets, and equipment to conserve power. A majority of respondents supported the idea of deactivating specific frequencies during outages to save energy instead or disabling technologies. However, some operators disagreed, citing concerns about quality of service degradation and lack of coverage in certain areas.

- Among operators, a small percentage stated they lack access to mobile emergency power equipment. The majority have different approaches to accessing such equipment, including SLAs with external suppliers, and owning their equipment.

- The questionnaire also addressed the use of renewable energy sources and half of the operators reported using them, with some relying on in-house systems, purchasing renewable energy, or having a primary supplier committed to renewables. Many adopt a flexible approach, combining renewables and conventional sources.

- Operators incorporate renewable energy sources into their infrastructure. Only a few use wind energy (up to 1% of network capacity), while solar energy is more prevalent. Solar

systems range from 1% to over 10% of their network capacity. Water-based energy sources are the least common.

- Some questions addressed customer dependency on a single connection or provider and roaming agreements. There was only a small number that have in place an approach for emergency situations.

- In relation to subsea cables, the majority of (traditional) operators do not own subsea cables and a significant number do not have direct interconnections with the external subsea cable providers. The ones that use them employ subsea cables as backup circuits, but many operators have not increased security nor introduced new measures in their contracts with subsea cable providers. These results alone do not provide a conclusive overview of the submarine cable landscape. The questionnaire made no distinction here as to whether countries are landlocked and whether operators are only active in such countries.

- A notable percentage of operators do not use satellite communication networks for their services. The key challenges identified vary among operators, but most were not aware of recent incidents in this context.

- **Technological Challenges, from Operators perspective**

In the survey answers to several key questions, the following insights emerge:

The majority of operators have implemented a range of measures to counteract phishing and vishing. These encompass preventive, detective, and reactive strategies. Preventive actions involve training and awareness campaigns, vital for recognizing fraudulent calls and SMS messages and responding effectively. Detective methods encompass diverse forms of traffic monitoring. Blocking mechanisms involve the utilization of firewalls to filter and block unwanted content.

- Regarding expectations from National Regulatory Authorities (NRAs) and other EU institutions about the NIS-2 Directive's implementation and integration into internal cybersecurity processes, the following insights emerge:

- Among the operators who responded, a majority expressed a positive outlook. They anticipate several forms of assistance like training and guidelines from relevant EU institutions on cybersecurity risk management measures and NIS-2 Directive's additional requirements; consultations, workshops, and industry feedback initiatives before new legislation enactment; support from national competent authorities and ENISA and last but not least expectations of cooperation and information exchange with NRAs on security-related matters, including NIS-2.

- A minority did not expect help in this regard, indicating that some processes are already underway with collaboration at the national level.

Overall, operators were largely hopeful for guidance, training, and collaborative efforts with authorities and institutions to effectively implement the NIS-2 Directive and adapt to cybersecurity processes. They emphasized the need for clear and transparent regulations and recommendations to support these endeavours.

- The data gathered on the utilization of national Internet Exchange Points (IXPs) for international traffic highlights a wide range of approaches to managing it. While a significant number of operators allocate around 5% of their traffic to national IXPs, there is no "one-size-fits-all" approach, with operators making these decisions based on their specific needs and opportunities for efficient traffic routing.

4.1 Findings

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

- On the IXPs:
    - Various deployments of the IXPs exist across the participating countries.
    - Very few countries perceive IXPs as cybersecurity enhancers.
    - The initial peek into the IXP topic showed strong differences in number of national IXPs among responding Countries. The diverse nature of the answers show it would be worthwhile for BEREC to further study the area of IXP.
- On the emergency power supplies (EPS):
    - Vast majority of operators have EPS in place for their entire core network
    - Backup times for EPS vary among the operators
    - Some operators are already using the energy saving procedures in emergencies
    - In 15 countries, there is some sort of regulation in place for EPS in mobile networks. Often it is targeting operators providing services for critical infrastructure.
    - The backup times where specified, ranged from 2 to 6 hours.
    - A significant majority of operators have access to mobile base stations that could be deployed to disaster-stricken regions when required.
- On the use of the renewable sources of energy and reduction of energy consumption:
    - Renewable energy sources are being introduced, mostly solar
    - Solar energy is used for up to 10% of the network energy needs
    - 68 out of 108 operators either have already taken steps or are considering implementing measures to reduce energy consumption
- On the subsea cables:
    - The majority of operators do not own subsea cables and a significant number do not have direct interconnections with external subsea cable providers

  - Many operators have not yet introduced increased security measures for their subsea connections
  - Many operators that have subsea cables use them as backup to increase resilience
  - 14 NRAs reported that they regulate subsea cables, and two of these have specific legal requirements for enhancing security in this field. 8 countries that have access to the sea do not regulate them.

- On satellite:
  - Among the operators that use satellite communications, tv broadcasting, internet access and voice services were the most common services provided using this type of communications.
  - Cybersecurity challenges for the satellite networks include ensuring data security, physical layer confidentiality, protection from electronic attacks such as jamming and spoofing, GPS/GNSS interference, malware and hacking protection, physical protection of satellites and base stations, lack of standardized security protocols, supply chain robustness.

- On NIS-2 Directive (NIS-2):
  - Regarding the NIS-2 implementation, operators have just undergone a significant effort to comply with the new national security and integrity legislation, therefore it would be useful to have a thorough and comprehensive listing of the additional requirements posed by the NIS-2 in this context.
  - There is a clear call to NRAs, BEREC, ENISA and the Commission to include stakeholders into the process for a consistent and harmonized implementation in the EU.
  - Most of the operators expect guidance and training by the relevant authorities as well as clear and transparent regulation and collaboration among all stakeholders.

- On the CPE and other customer customer-related security measures:
  - Security legislative requirements for CPEs or other end users' devices are in place in 6 countries
  - The highest ranked security measures for the CPE equipment mentioned by the operators include automatically configured firewalls, device hardening, patch management, bug fixing, manufacturing stage penetration testing, isolation of traffic, encryption security protocol protection, managed authentication requirements for access and implemented endpoint security solution.

- On smishing and vishing:

- 62 operators mention having measures in place to prevent smishing and vishing attacks. These include preventive, detective and reactive measures. Among them explicitly mentioned were voice and SMS spam firewalls (including AI-based solutions) and filtering at the signalling level (e.g. DIAMETER and SS7).

- On mitigating DDos attacks:
  - Majority of operators use DDoS protection through internal and/ or external platforms. Measures mentioned to mitigate DDoS attacks include anti DDoS protection on multiple layers, administrative measures, routing modification, firewalls and port blocking, network segmentation/isolation and zoning, limiting the number of concurrent sessions, cloud-based scrubbing and blackhole routing as last resort.

4.2 Open issues and possible future work

- How to provide power supplies in emergency situations caused by natural disasters e.g. floods or earthquakes.
- Energy consumption reduction, promoting the use of sustainable energy sources.
- Further investigate IXP landscape and its' role in strengthening national resilience.
- NIS-2 transpositions in the EU – impact on the markets.
- CPE cybersecurity related issues.

5 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 NIS-2 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 %)

	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?
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?**

	Dependencies on other infrastructures
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

Annex 4 – Links to National Legislation

NRA	Link/Info
ANCOM	IXPs are DSP and are regulated under law 362/2018: https://legislatie.just.ro/Public/DetaliiDocument/209670
BNETZA	The German Telecommunication Act is just available in German: https://www.gesetze-im-internet.de/tkg_2021/inhalts_bersicht.html
ECOI	https://www.althingi.is/lagas/nuna/2019078.html
DBA	https://www.retsinformation.dk/eli/lta/2018/437
OCECPR	https://dsa.cy/images/pdf-upload/Decision-389-2020.pdf
UKE	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
ACM	Wbni: https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen
CNMC	https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757
NMHH	249/2017. (IX. 5.) government decree on the identification, assignment and protection of critical infrastructures in the telecommunications sector (https://nki.gov.hu/wp-content/uploads/2020/11/Gov.Dec_.-249_2017-on-ICT.pdf)
ILR	https://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo
RTR	NIS Act: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536 NIS Ordinance: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722
ComReg	SI 360 of 2018
TRAFICOM	For example chapters 29 and 33 of Act on Electronic Communications Services
AGCOM	IXPs are under the NIS Directive (Directive EU 2016/1148), which has been transposed into national legislation with the Legislative Decree n. 65 of 2018 and subsequent notifications (notably Law Decree 82 of 2021, which established the National Cybersecurity Agency (ACN), centralizing there the NIS competent authority, the single point of contact and the CSIRT)
RATEL	https://www.ratel.rs/en/page/laws-electronic-communications

Annex 5 – List of figures

Figure 1 Is there any legal obligation for operators regarding emergency power supply in mobile networks in your country? 5
Figure 2 Legal obligation for the access network and/or core network 6
Figure 3 Regulation of subsea cables 7
Figure 4 Location of existing and planned subsea cables 8
Figure 5 Type of information available on individual subsea cables 8
Figure 6 Documentation of subsea cables 9
Figure 7 Framework regulating IXPs 10
Figure 8 Permanent emergency power equipment in networks 12
Figure 9 Duration of emergency power supply 13
Figure 10 Access to mobile emergency power equipment 14
Figure 11 Access to mobile base stations for distribution to disaster regions 15
Figure 12 Solutions to avoid dependencies 17
Figure 13 Ownership of externally provided subsea cables 18
Figure 14 Methods to ensure resilience over subsea cable connections 19
Figure 15 Increased security or introduction of new security measures since last year 19
Figure 16 Types of Satellite Communication Networks Services 21
Figure 17 Percentage of international traffic going through national IXPs 25