BEREC
Body of European Regulators for Electronic Communications

BoR (22) 197

# Report on ECA Audit recommendations for 5G cybersecurity

December, 2022

# Contents

# Executive Summary

The BEREC 5G Cybersecurity Working Group prepared an internal BEREC report in October 2021 based on the information collected through the questionnaire prepared by the European Court of Auditors (ECA). The questionnaire for NRAs sought for their view on whether the EU and its Member States are rolling out secure 5G networks in a timely and concerted manner.

In January 2022 the ECA issued Special Report 03/2022: 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved issued (Special Report). The Special Report calls for new impetus to boost the roll-out of 5G, the new global wireless standard for mobile networks, in the EU. It provides insights and recommendations for the timely deployment of secure 5G networks across all the EU countries.

BEREC analysed the ECA's Recommendations aiming at providing its views and proposals for future actions to help with the Recommendations implementation.

In this report, BEREC presents its past activities that are related to some of the recommendations formulated by the ECA.

While the implementation of the recommendations is the responsibility of the Commission and the NIS Cooperation Group, some preliminary proposals on possible BEREC activities to support the European Commission and the NIS Cooperation Group with the security-related recommendations are presented in this report.

BEREC will streamline its activities with all other stakeholders addressed namely ENISA, the European Commission and the NIS Cooperation Group which is leading the activities on 5G security and the 5G Toolbox.

# 1. Context

This chapter provides some background information for the European Court of Auditors' (ECA) Special Report 03/2022: 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved (Special Report) and BEREC's contribution to this Special Report.

The ECA has conducted an audit that assessed whether the European Commission and the Member States (MS) rolled out secure 5G networks in a timely and concerted manner. It also examined the European Commission's support for Member States in 5G set-up.

The audit covered the period between 2016 and May 2021 and focused on the 5G policy framework at EU level, the European Commission's activities and on the implementation by the Member States of the 5G action plan and of the EU toolbox on 5G cybersecurity (hereafter the 5G toolbox). It also considered the Commission's warning about the dependencies of many critical services on 5G networks would make the consequences of widespread disruption particularly serious.

The ECA examined whether the Commission effectively supported Member States in achieving EU objectives for the roll-out of their 5G networks and addressing 5G security concerns.

It is to be noted that the ECA publications – audit reports, reviews and opinions – are an essential element of the EU's accountability chain. They help the European Parliament and the Council to monitor and scrutinise the achievement of the EU's policy objectives, and to hold to account those responsible for managing the EU budget, principally the European Commission.

The BEREC 5G Cybersecurity Working Group, supported the ECA in the audit process and drafted an *Internal Report* based on the information collected through the questionnaire prepared by the ECA.

In general, the answers show that NRAs think that the Commission and the Member States have taken the necessary steps to implement secure 5G networks in a timely and concerted manner. The answers indicate that there is still some room for improvement when it comes to a common understanding of the terminology and the identification of the roles of the different actors involved in the implementation of secure 5G networks.

Following the audit, the ECA also created a Special Report which was published in January 2022. The aim of the report was to provide insights and recommendations for the timely deployment of secure 5G networks across all the EU countries.

In the Special Report, the ECA noted some considerable delays in the Member States deployment of 5G networks (cf. no. 81 ECA report).

The ECA highlighted that there is a need for further considerations such as on criteria for classifying 5G vendors as high-risk (cf. no. 91).

In June 2022 the Council of the EU published the Council conclusions on the Special Report.

The Council invites the Member States and the Commission to pay attention to the recommendations of the Special Report and encourages them to consider those recommendations when elaborating their policies on the development of their 5G networks while ensuring the security of those networks by the application and further development of the 5G cybersecurity toolbox, in light of new security issues emerging from technological trends and developments in the 5G supply chain.

The Council also invites the Commission, with the support of ENISA, and the Member States to continue the coordinated EU-cooperation on the 5G security measures and the monitoring of the implementation of the 5G cybersecurity toolbox and to assess the need for a more homogeneous approach to the use of its elements.

BEREC announced in their latest report to analyse the final report of the ECA and examine how it can support the Commission and NIS Cooperation Group in the implementation of the recommendations in the future.

In this Report, BEREC presents its views on the ECA's Recommendation. The Audit focused on the Commission, but the ECA also examined the role of National Administrations and other actors.

## 2. Conclusions and recommendations

Overall, the Audit carried out by the ECA indicated some very important issues that need to be addressed promptly in order not to derail Commission's 2016 5G Action Plan. These issues are

- Considerable delays in the Member States deployment of 5G networks despite Commission's support.
- Further efforts are necessary to address security issues in 5G deployment.
- Deviation from the Commission's 2025 and 2030 targets on 5G coverage of all urban areas and along main transport paths, and full coverage, respectively. Although most MS achieved the intermediary objective of having at least one major city with access to such services, not all of them refer to the Commission's objectives in their national Strategies.
- In several MS, the EECC has not been yet transposed in national law and 5G spectrum awards were delayed, mostly due to weak demand as for example in the case of mm-wave band spectrum, cross-border coordination issues, impact of the pandemic and uncertainty on how to deal with security issues.
- Lack of a definition of the expected quality of service of 5G networks (speed and latency related KPIs) by the Commission. Therefore divergent approaches by MS are observed. This might create a risk of inequalities in the access and quality of 5G Services across the EU, thus increasing the digital divide and also affecting the functioning of the EU single market.
- Since the Toolbox was adopted, progress has been made to reinforce the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors.
- However, Member States have applied divergent approaches regarding the use of equipment from high-risk vendors or the scope of the restrictions. The ECA concluded that there is a risk that the Toolbox in itself cannot guarantee that Member States address security aspects in a concerted manner.

In order to address the above issues, the ECA proceeded to the following recommendations which should be satisfied by December 2022:

1) In order to promote the even and timely deployment of 5G networks within the EU the Commission should

   a) together with MS develop common definition of QoS parameters of 5G Networks (minimum speed and maximum latency).

b) encourage MS to include Commission's 2025 and 2030 objectives and measures needed to achieve them in their next updates of their strategies.

c) support MS in addressing spectrum coordination issues with neighbouring non-EU-countries by keeping it on the agenda of every relevant meeting.

2) In order to address the divergent approach by MS in applying the security measures for high risk vendors of 5G and ensuring that business providing services to EU citizens respect the EU rules and values, the Commission should

a) provide further guidance or support actions on key elements of the EU toolbox on 5G Cybersecurity, such as criteria for assessing 5G vendors and classifying them as high-risk and on data protection considerations.

b) promote transparency on the Member States' approaches to 5G security, by monitoring and reporting on the implementation of the security measures of the EU toolbox on 5G cybersecurity. This should be done using a common set of key performance indicators.

c) together with Member States, assess for which aspects of 5G networks security there is a need for specifying enforceable requirements and, where appropriate, initiate legislation

3) In order to monitor MS's approaches towards 5G security and assess the impact of divergences on the effective functioning of the single market, the Commission should

a) promote a transparent and consistent approach regarding the Member States' treatment of MNOs' costs for replacing 5G equipment purchased from high-risk vendors by regularly monitoring and reporting on this issue within the implementation of the EU toolbox on 5G cybersecurity

b) assess what the impact on the single market would be of a Member State building its 5G networks using equipment from a vendor considered to be high-risk in another Member State

# 3. Relevant BEREC's past activities

In the past years BEREC has conducted multiple activities which may be relevant for the recommendations of the ECA.

These activities and related deliverables are listed here with a short description.

## 3.1. For Recommendation 1 (a)

Recommendation 1 (a) together with Member States, develop a common definition of the expected quality of service of 5G networks, such as the performance requirements it should offer in terms of minimum speed and maximum latency;

BoR(20) 33 Feasibility study on development of coverage information for 5G deployments

BEREC set out to consider the feasibility of provisioning coverage information and Quality-of-Service (QoS) aspects of future 5G networks that cater for the needs of verticals. The objective was to provide insights on two key areas:

1) Describe the expected benefits from NRAs' presentation of coverage information and QoS aspects for use by verticals implementing use cases such as automotive, industrial, environmental monitoring, etc;
2) Attempt to describe the metrics that are of relevance to the verticals.

In addition, BEREC sets out its conclusion and recommendation in light of the practical difficulties of determining the merits of the project.

BoR (21) 163 Summary report on BEREC Workshop on "NRA experiences with 5G"

BEREC conducted a workshop for experts on 23 September 2021 to continue to develop an understanding of how service availability in mobile networks using 5G technology can be predicted/calculated. One main objective of the workshop was to build a collective appreciation of how to manage generating information to users on 5G such that there would not be a wide gap between predicted and actual service/experience levels in terms of coverage. The workshop was an internal forum for experts to exchange relevant experiences.

## 3.2. For Recommendation 2 (b)

Recommendation 2 (b) promote transparency on the Member States' approaches to 5G security, by monitoring and reporting on the implementation of the security measures of the EU toolbox on 5G cybersecurity. This should be done using a common set of key performance indicators (KPIs).

BoR (20) 227 Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)

This Report was created as an Internal BEREC document, and as an input to the NIS Cooperation Group as part of its review of the implementation of the 5G Toolbox across the EU.

BoR (20) 228 Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)

The BEREC Report provides an overview on the state of play of the implementation of the EU 5G Cybersecurity Toolbox (herein: 5G Toolbox) strategic measures: SM05 - Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies - and SM06 - Strengthening the resilience at national level. This data was collected following the invitation of the NIS Cooperation Group and has been used as input to the Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks.

Joint ENISA-BEREC Workshop on 5G cybersecurity toolbox developments and way(s) forward

On 21 December 2020, BEREC together with ENISA held a workshop under the title "5G cybersecurity toolbox developments and way(s) forward" via web-streaming.

The event was opened by Dan Sjoblom, BEREC Chair 2020, Juhan Lepassaar, Executive Director of ENISA and Lorena Boix Alonso, Director of Digital Society, Trust and Cybersecurity Directorate of the European Commission.

The workshop explored the following areas:

1) EU-wide 5G Cybersecurity toolbox implementation process (EC, DG CNECT H)
2) Implementation of the 5G Cybersecurity toolbox Technical Measures (ENISA)
3) 5G Cybersecurity toolbox Strategic Measures 5 and 6 – a market and regulatory perspective (BEREC)

BoR (22) 89 An overview of the BEREC work on the national resilience of network operations

In order to gain a better understanding on national resilience, BEREC drafted two separate questionnaires to collect relevant information from the market players and national authorities (NRAs). Both surveys provide insights into the national resilience by examining the organisation and operation of the security related functions within the MNOs' networks.

BEREC analysed all responses gathered and prepared an internal report. The results are not made public due to the confidentiality and sensitivity of the responses received from the MNOs and NRAs.

The results obtained from the MNO survey allow BEREC to gain insights in how a significant number of MNOs in the EU organise these important security related network functions, in particular whether these are operated internally or outsourced and where they are located.

The survey for NRAs allows BEREC to identify the countries with current or planned legislation that imposes requirements on how the MNOs operate security related functions within their network

## 3.3. For Recommendation 3 (a)

Recommendation 3 (a): "promote a transparent and consistent approach regarding the Member States' treatment of MNOs' costs for replacing 5G equipment purchased from high-risk vendors by regularly monitoring and reporting on this issue within the implementation of the EU toolbox on 5G cybersecurity."

The documents BoR (20) 227 and BoR (20) 228 are also relevant for Recommendation 3 (a).

BEREC undertook a first step to examine the deployment, the opportunities and challenges and the costs of replacing equipment in its work on Open RAN.

BoR (21) 162 BEREC Internal Report on the Open Radio Access Network (RAN)

Open RAN is a possible evolution in the technological development of communications networks. Although Open RAN is not explicitly mentioned in the EU toolbox on 5G Cybersecurity, it is perceived as a tool to implement some of the measures in the toolbox, notably strategic measure 5 related to the diversification of suppliers.

BEREC conducted a survey of the opinion of MNOs on certain aspects of Open RAN. The general areas covered in the survey included the areas of focus and interest, the maturity level, the standardization and certification, the motivation and challenges for deployment and the impact on cost.

BEREC analysed the survey responses and drafted an internal BEREC report where the survey results are complemented by BEREC's observations on the predominant opinions expressed by MNOs on each area of the survey. An internal-only report was developed, due to the confidentiality and sensitivity of the responses received from the MNO's. In the Conclusions chapter BEREC puts forward the main findings, the open issues observed and a possible way forward.

BoR (22) 23 An overview of the BEREC work on the Open Radio Access Network (RAN)

The findings, open issues observed and possible way forward formulated in the internal report are published in this overview.

BEREC identifies a need to establish a greater understanding of the commercialization path of Open RAN deployments, the opportunities this will bring, as well as the need to investigate further how challenges associated with Open RAN are being addressed by stakeholders other than MNOs (vendors, service providers, policy makers, testing facilities, etc.).

BoR (22) 138 Summary Report: BEREC Open RAN workshop

On 24 May 2022 BEREC conducted an external workshop on Open RAN. The purpose was to develop an understanding of the concept of mobile infrastructure deployment and development using Open RAN.

BEREC invited expert speakers from regulators, policy makers and industry to explore potential future areas of enquiry for BEREC.

This summary report is not intended to be a transcript of the workshop, but provides some transparency as to the nature of the discussions during the workshop sessions for interested parties. It sets out the main attendee material.

# 4. Non-exhaustive list of potential initiatives

The BEREC 5G Cybersecurity WG has reviewed the recommendations of the ECA in the Special Report and is of the view that BEREC could have a role to support the Commission and the NIS Cooperation Group with regards to some of these recommendations.

This chapter contains a non-exhaustive list of potential initiatives for some of the recommendations related to 5G Cybersecurity. Possible initiatives related to the deployment of 5G networks within the EU (Recommendation 1) are not considered in this list.

## 4.1. For Recommendation 2 (b)

Recommendation 2 (b) promote transparency on the Member States' approaches to 5G security, by monitoring and reporting on the implementation of the security measures of the EU toolbox on 5G cybersecurity. This should be done using a common set of key performance indicators (KPIs).

The 5G EU toolbox of risk mitigating measures describes strategic measures (SM) on the diversification of suppliers:

- SM05: Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies
- SM06: Strengthening the resilience at national level

These measures ensure the diversity of supply within each operator and geographical balance at national level. The expected effectiveness of these measures to treat the risk of dependency on a single supplier depends on the scope of the measures but can be 'very high' according to the classification in the risk mitigation plans of the toolbox. The measure is considered effective to a very high degree, meaning that it is expected to almost completely mitigate the related risks. The indicative timeframe was short to medium term, so up to 5 years.

Amongst the technical measures (TM) in the 5G EU toolbox of risk mitigating measures, there is TM05 about ensuring secure 5G network management, operation and monitoring. This includes ensuring that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU and that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.

BEREC could in cooperation with the Commission and NIS Cooperation Group identify which indicators may be used to measure the effectiveness of the implementation of the security measures related to SM05, SM06 and TM05. This work could be based on BEREC's past work described in the previous chapter.

The most relevant indicators could be used as a common set of KPIs. BEREC can study the possibility to complement the monitoring activities by the Member States in the NIS Cooperation Group. This could be done by periodically collecting information from the providers and NRAs.

## 4.2. For Recommendation 2 (c)

Recommendation 2 (c) together with Member States, assess for which aspects of 5G networks security there is a need for specifying enforceable requirements and, where appropriate, initiate legislation.

To foster a concerted approach to 5G security among Member States, BEREC could help with collecting information from the NRAs. To gather the relevant information the different aspects of the 5G networks security need to be identified first. This work could be done in collaboration with ENISA and the NIS CG. Based on these initial findings further efforts could be put into identifying enforceable requirements from the 5G Toolbox that can be further specified and implemented in all Member States.

If requested by the Commission or NIS Cooperation, BEREC could examine the current situation or practices in Members States or practices or policies used by the providers. This can be done through surveys, interviews, workshops, etc.

BEREC could also follow-up on the initiatives to develop security measures guidelines and legislation, for example under the EECC or upcoming NIS2 framework. Where relevant, BEREC could help the Commission, ENISA and the NIS CG with the collection of information from NRAs or providers.

## 4.3. For Recommendation 3 (a)

Recommendation 3 (a): “promote a transparent and consistent approach regarding the Member States’ treatment of MNOs’ costs for replacing 5G equipment purchased from high-risk vendors by regularly monitoring and reporting on this issue within the implementation of the EU toolbox on 5G cybersecurity.”

The BEREC 5G Cybersecurity WG ran a Survey in 2020 where it investigated the advantages or the main reasons for implementing diversity of suppliers at national level. The responses collected from NRAs showed that the main advantages for implementing diversity of suppliers in their view were in avoiding potential network equipment failure and discontinuation of the service provision. The possibility to quickly refrain from using equipment of a specific supplier in the network(s) would be beneficial in case of supply chain disruption, detected security

vulnerabilities, and also for economic or strategic reasons (national security in general). It was obvious that the ability to switch suppliers (so as to avoid a lock-in scenario) was regarded as very important and beneficial by the vast majority of relevant national authorities. BEREC therefore asked MNOs about the time needed to replace specific equipment or implement multi-vendor strategy in different parts of their networks without significant economic impact. With this question, BEREC was aiming at finding out the equipment replacement lifecycle in existing networks.

To tackle this recommendation there first needs to be an understanding of:

- Current 5G deployment status of MNO's in each Member State;
- 5G deployment plans of MNO's in each Member State by 2025;
- Current and planned choice of 5G vendors (for RAN, Transport, Core and Edge) by the MNO's in each Member State;
- The replacement cycle of the 5G equipment for RAN, Transport, Core and Edge.

BEREC could undertake an initiative to survey MNOs across the Member States on some of the above points. In the past years BEREC already collected information about the vendors and their origin (EU or non-EU) in commercial networks of different generations for the report BoR (20) 227. BEREC collected preliminary information about the costs and timeframe for deploying Open RAN for the report BoR (21) 162. A similar approach focused on vendors diversification and deployment timeframe could be followed here.

BEREC could then compile the results of such a survey into a report. This report could be an input for the work of the NIS Cooperation Group related to the monitoring of the deployment of 5G equipment in the Member States.

# 5. Conclusion

BEREC reviewed the recommendations produced by the ECA and identified where BEREC could support the Commission. BEREC is of the view that it could support the Commission with the following recommendations related to security:

- 2 (b) by proposing KPIs for SM05, SM06 and TM05.
- 2 (c) by studying any proposal made by the Commission and where relevant collect information from NRAs and providers.
- 3 (a) by examining how BEREC can contribute to an evaluation of the deployment of 5G equipment and the replacement cycle of 5G equipment.