



EUROPEAN
COURT
OF AUDITORS

Audit preview

Information on an upcoming audit



Implementing secure 5G networks in the EU and its Member States

December 2020

5G, the fifth generation of mobile and wireless telecommunication systems, marks a revolutionary advance on its predecessors (3G and 4G). It offers ultra-high-speed connection, supporting a high number of connected devices and objects ("internet of things"). 5G will affect many aspects of EU citizen's life, such as e-health, smart cars and smart electricity networks.

The way 5G is deployed across the EU will therefore be important for the effective functioning of the single market and Europe's digitalisation efforts. In particular, delays in achieving an appropriate 5G coverage, as well as 5G security issues, may have huge implications for the EU's competitiveness and strategic independence.

The ECA is currently conducting an audit to assess whether the EU and its Member States are implementing secure 5G networks in a timely and concerted manner. This follows on from its review, published earlier this year, of the EU's response to China's state-driven investment strategy, which also flagged 5G security as an issue of concern. In particular, it highlighted the lack of a concerted approach among Member States and the use of Chinese 5G equipment in critical EU infrastructure.

We will examine the EU's 5G set-up, the support provided to the Member States by the Commission, and the Member States' implementation of 5G, especially their consideration of security concerns.

"Implementation" refers both to the development of the framework (such as legislative or regulatory measures), and to the deployment of the physical infrastructure, e.g. antennas and broadband.

If you wish to contact the audit team, you may do so at the following email address:

ECA-5G-audit@eca.europa.eu

Contents

What is 5G and why is it important?	4
Legal framework	5
Roles and responsibilities	7
Why carry out an audit on 5G security, and why now?	8
Focus of the audit	9

What is 5G and why is it important?

What is 5G?

The term 5G refers to the fifth generation of mobile and wireless telecommunication systems. It marks a revolutionary advance on its third- and fourth-generation predecessors (3G and 4G), even though 5G networks will retain some elements of those technologies. It offers ultra-high-speed connection, supporting a high number of connected devices and objects ("internet of things"). 5G will affect many aspects of life for people in the EU, through developments such as e-health, smart cars and smart electricity networks.

Picture 1 – 5G: an overview



Source: European Commission, <https://ec.europa.eu/digital-single-market/en/towards-5g>.

Why is it important for the EU?

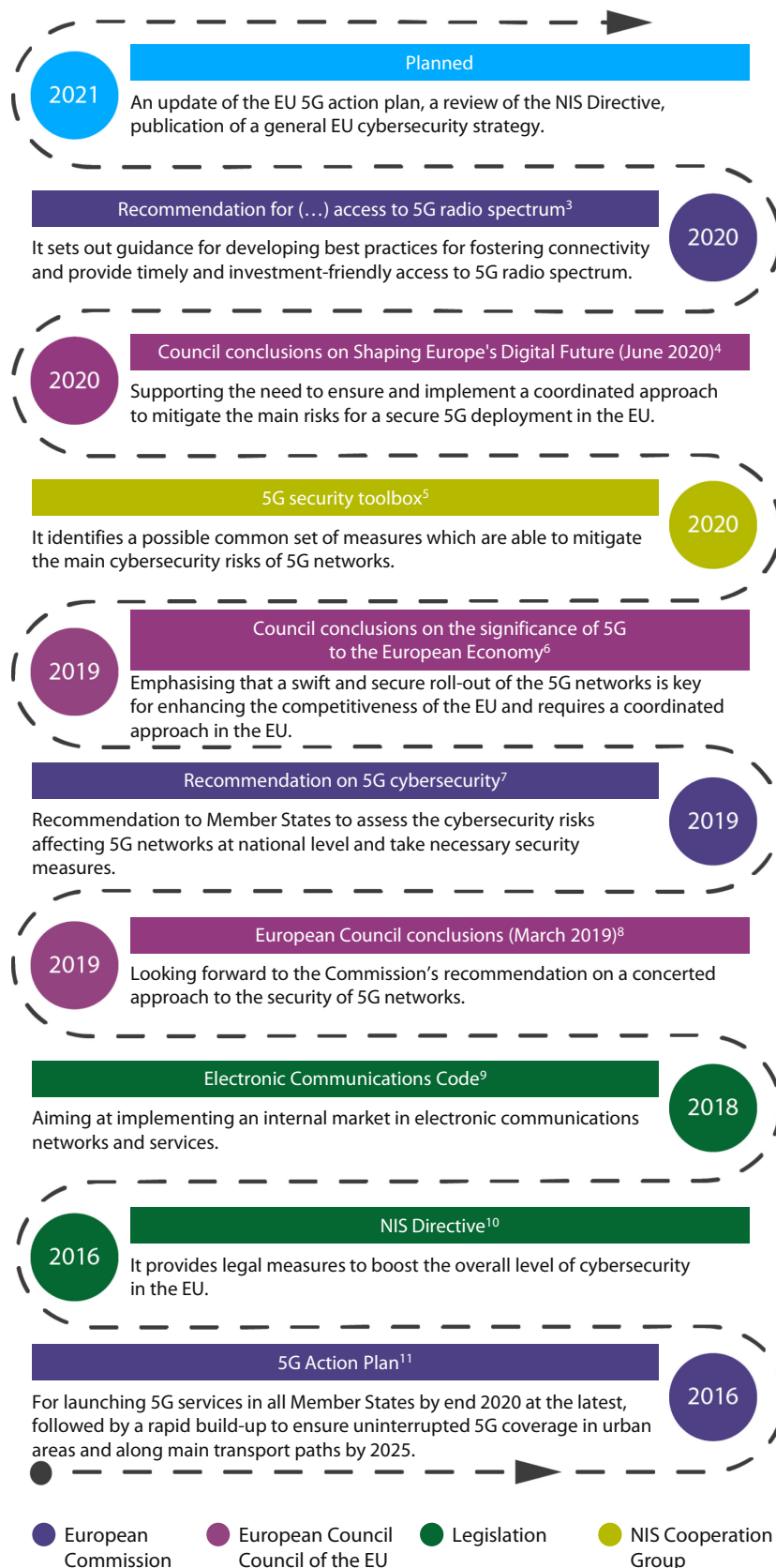
5G will be one of the most critical building blocks of our digital economy and society in the next decade and beyond. It will serve a wide range of applications and industries, becoming strategically important for the entire EU single market. A study carried out on behalf of the European Commission indicates that introducing 5G across four key strategic industries (automotive, health, transport and energy) may generate as much as €113 billion per year¹, and that 5G investment is likely to create 2.3 million jobs in the Member States.

However, this is not the only reason 5G demands an EU-wide approach. Both 5G infrastructure and potential threats to its security are of a cross-border nature. Therefore, any significant vulnerabilities and/or cybersecurity incidents concerning 5G networks in one Member State would affect the EU as a whole. Cybersecurity is also an area of concern for many people in the EU².

Legal framework

The EU legal framework relating to 5G networks and 5G security is varied and complex. The most relevant part consists of “soft” law, such as Commission recommendations and communications. [Figure 1](#) provides an overview.

Figure 1 – Most relevant policy and legal documents



Source: ECA.

EU funding

EU funding for 5G has come mainly from the European Fund for Strategic Investments (EFSI), the European Fund for Regional Development (ERDF) and Horizon 2020, the EU's eighth research framework programme:

- **EFSI**: financed two 5G-related projects for a total of €1 billion¹².
- **ERDF**: contributed at least €147 million to 5G projects¹³.
- **Horizon 2020**: contributed about €614 million to 5G projects¹⁴.

Between 2016 and 2020, the period covered by the audit, the EIB also signed eight loan agreements providing a total of €1.765 billion of its own resources for 5G projects in five Member States¹⁵.

There is no specific EU funding related to 5G security in the 2014-2020 period.

Roles and responsibilities

At EU level

The **European Commission** supports and coordinates action by Member States in relation to technical and security aspects of 5G networks. Within the Commission, responsibility for 5G policy, including security, lies primarily with the Directorate-General for Communications Networks, Content and Technology (**DG CONNECT**). It manages 5G funding under Horizon 2020 and coordinates other DGs and EU bodies that play a role in 5G policy development and implementation (see below).

Insofar as 5G projects can also be funded under cohesion policy, the Directorate-General for Regional and Urban Policy (**DG REGIO**) also plays a role.

In addition, the **European Investment Bank** (EIB) finances 5G projects, both through its own funding and through the European Fund for Strategic Investments (EFSI). It provides loans to the telecom sector as a whole, including for 5G activities.

The **NIS cooperation group** serves a forum as for strategic cooperation and information exchange among EU Member States on cybersecurity (including 5G network security).

ENISA is involved in establishing European cybersecurity certification schemes.

In the Member States

National authorities (e.g. Ministries for Telecommunications) are responsible for developing and implementing their national 5G plans and ensuring security. Under the NIS directive¹⁶, Member States should adopt a national strategy for secure network and information systems. By the end of September 2020, 5G commercial services had been rolled out in 17 EU Member States (Austria, Belgium, Bulgaria, Czech Republic, Denmark, Finland, Germany, Hungary, Ireland, Italy, Latvia, Netherlands, Poland, Romania, Slovenia, Spain and Sweden) plus the UK¹⁷.

Telecom operators themselves are responsible for the rollout of secure 5G networks, using equipment from technology vendors. According to a study from November 2019¹⁸, several such vendors hold or have applied for patents in the 5G industry. The main ones are China's Huawei (16 %) and ZTE (10 %), Europe's Nokia (11 %) and Ericsson (7 %), the USA's Qualcomm (6 %) and Intel (4 %), South Korea's Samsung (14 %) and LG (12 %) and Japan's Sharp (4 %) and NTT Docomo (4 %).

Why carry out an audit on 5G security, and why now?

In the years to come, the way 5G is deployed across the EU will be important for the effective functioning of the single market and Europe's digitalisation efforts. In particular, delays in achieving an appropriate 5G coverage as well as 5G security issues may have huge implications for the EU's competitiveness and strategic independence. Furthermore, considerable EU funding has been allocated to 5G projects in recent years (see "EU funding").

The audit follows on from [ECA Review No 3/2020](#) on the EU's response to China's state-driven investment strategy, which highlighted the use of Chinese 5G equipment in critical EU infrastructure and the lack of a concerted approach to 5G security among Member States as issues of concern.

The audit also follows the Commission's recommendation on 5G security in March 2019, and the adoption of the EU toolbox on 5G cybersecurity in January 2020. This year also marks a major milestone in the implementation of the 5G Action Plan, adopted in 2016 (see [Figure 1](#)): by the end of 2020 at the latest, 5G services were due to have been launched in all Member States.

Focus of the audit

The purpose of the audit is to assess **the implementation of secure 5G networks in the EU and its Member States**. In particular, we will examine whether:

- the EU's 5G set-up is conducive to the implementation of secure 5G networks across Member States;
- the Commission has provided Member States with the necessary support; and
- Member States are implementing secure 5G networks in a timely and concerted manner.

The audit will focus on 5G network security, encompassing cybersecurity and hardware security. We will cover actions taken since 2016 and examine data gathered in four Member States (Finland, Germany, Poland and Spain).

The audit **will not** cover matters relating to the **safety** of 5G, such as its potential impact on human and animal health or the environment.

ABOUT ECA SPECIAL REPORTS AND AUDIT PREVIEWS

The ECA's special reports set out the results of its audits of EU policies and programmes or management topics related to specific budgetary areas.

Audit previews provide information in relation to an ongoing audit task. Since we identified the issues underlying these areas of enquiry before the audit work commenced, they should not be regarded as audit observations, conclusions or recommendations. They are based on preparatory work undertaken before the start of the audit and are intended as a source of information for those interested in the policy and/or programme being audited.

If you wish to contact the team in charge of this audit, please do so through the following e-mail address:

ECA-5G-audit@eca.europa.eu

-
- 1 Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, February 2017.
 - 2 Special Eurobarometer 499 – “Europeans’ attitudes towards cybersecurity”, January 2020.
 - 3 Commission recommendation of 18.9.2020 on a common Union toolbox for reducing the cost of deploying very high capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the COVID-19 crisis in the Union.
 - 4 [Council conclusions of 9 June 2020](#) on shaping Europe’s digital future.
 - 5 [Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures](#). NIS cooperation group, 01/2020.
 - 6 [Council Conclusions of 3 December 2019](#) on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G.
 - 7 [Commission recommendation \(EU\) 2019/534](#) of 26 March 2019 Cybersecurity of 5G networks.
 - 8 [Council’s conclusions of 22 March 2019](#) on a concerted approach to the security of 5G networks.
 - 9 [Directive \(EU\) 2018/1972](#) of the European Parliament and of the Council of 11 December 2018 on establishing the “European Electronic Communications Code”.
 - 10 [Directive \(EU\) 2016/1148](#) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
 - 11 COM(2016)588, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 5G for Europe: An Action Plan.
 - 12 <https://www.eib.org/en/projects/pipelines/all/20170792> and <https://www.eib.org/en/projects/pipelines/all/20180099>.
 - 13 Links to the different managing authorities’ websites can be found in [Dataset of projects co-funded by the ERDF during the multi-annual financial framework 2014-2020](#), J. Bachtrögler, M. Doussineau and P. Reschenhofer; Publications Office of the European Union; Luxembourg, 2020; ISBN 978-92-76-18860-5, doi:10.2760/491487, JRC120637.
 - 14 <https://webgate.ec.europa.eu/dashboard/sense/app/93297a69-09fd-4ef5-889f-b83c4e21d33e/sheet/a879124b-bfc3-493f-93a9-34f0e7fba124/state/analysis>.
 - 15 <https://www.eib.org/en/projects/loans>.

-
- ¹⁶ [Directive \(EU\) 2016/1148](#) of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- ¹⁷ <http://5gobservatory.eu/wp-content/uploads/2020/10/90013-5G-Observatory-Quarterly-report-9-V2.pdf>.
- ¹⁸ [Who is leading the 5G patent race? IPlytics Platform, November 2019](#). The study lists the number of declared 5G patent families by company name.

COPYRIGHT

© European Union, 2020.

The reuse policy of the European Court of Auditors (ECA) is implemented by Decision of the European Court of Auditors No 6-2019 on the open data policy and the reuse of documents.

Unless otherwise indicated (e.g. in individual copyright notices), the ECA's content owned by the EU is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence. This means that reuse is allowed, provided appropriate credit is given and changes are indicated. The reuser must not distort the original meaning or message of the documents. The ECA shall not be liable for any consequences of reuse.

You are required to clear additional rights if a specific content depicts identifiable private individuals, e.g. in pictures of the ECA's staff, or includes third-party works. Where permission is obtained, such permission shall cancel and replace the above-mentioned general permission and shall clearly indicate any restrictions on use. To use or reproduce content that is not owned by the EU, you may need to seek permission directly from the copyright holders. Software or documents covered by industrial property rights, such as patents, trade marks, registered designs, logos and names, are excluded from the ECA's reuse policy and are not licensed to you.

Cover page – Shutterstock / 620247719

The European Union's family of institutional Web Sites, within the europa.eu domain, provides links to third-party sites. Since the ECA has no control over them, you are encouraged to review their privacy and copyright policies.

Use of European Court of Auditors' logo

The European Court of Auditors logo must not be used without the European Court of Auditors' prior consent.