EN 2022

03

Special Report

5G roll-out in the EU:

delays in deployment of networks with security issues remaining unresolved

CURIA RATIONUM

EUROPEAN
COURT
OF AUDITORS

Contents

Executive summary

I The "fifth generation" of telecommunication systems, or 5G, is a new global wireless standard that offers a much higher data capacity and transmission speeds. 5G services are essential for a wide range of innovative applications which have the potential to transform many sectors of our economies and improve citizens' daily lives. 5G is therefore of strategic importance for the entire single market.

II In its 2016 5G Action Plan, the Commission put forward the objective of ensuring uninterrupted 5G coverage in urban areas and along main transport paths by 2025. In March 2021, it extended the objective to include 5G coverage of all populated areas by 2030.

III While 5G has the potential to unleash many opportunities for growth, it comes with certain risks. In its 2019 recommendation on 5G cybersecurity, the Commission warned that the reliance of many critical services on 5G networks would make the consequences of widespread disruption particularly serious. Furthermore, owing to the cross-border nature of threats involved, any significant vulnerability or cybersecurity incidents in one Member State would affect the EU as a whole. One of the outcomes of the Commission recommendation was the EU toolbox on 5G cybersecurity ("toolbox"), which was adopted in January 2020.

IV Across the EU, the total cost of 5G deployment could reach €400 billion. In the 2014-2020 period, the EU provided funding of over €4 billion for 5G projects.

V We 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 in a concerted manner. We assessed aspects related to both the implementation of 5G networks, for which 2020 was a key year, and their security. The aim of this report is to provide insights and recommendations for the timely deployment of secure 5G networks across all the EU countries. Our audit focused on the Commission, but we also examined the role of national administrations and other actors.

VI Our audit showed that there are delays in Member States' roll-out of 5G networks. By the end of 2020, 23 Member States had launched commercial 5G services and achieved the intermediate objective of at least one major city with 5G access. However, not all Member States refer to the EU's 2025 and 2030 objectives in their national 5G strategies or broadband plans. Moreover, in several countries the European Electronic Communications Code has not yet been transposed into national law and the assignment of 5G spectrum has been delayed. These delays in assigning the spectrum can be attributed to different reasons: a weak demand by Mobile Network Operators (MNOs), cross-border coordination issues with non-EU countries along the eastern borders, the impact of COVID-19 on the auction schedules and uncertainty about how to deal with security issues. The extent to which Member States are lagging behind on 5G implementation puts the achievement of the EU objectives at risk. The Commission has provided Member States with support for implementing the 2016 5G Action Plan through both hard and soft law initiatives, guidance and the funding of 5G-related research. However, the Commission has not clearly defined the expected quality of 5G services.

VII The EU toolbox on 5G cybersecurity specifies a number of strategic, technical and support measures to deal with 5G network security threats and identifies the relevant actors for each of these measures. Several measures address the issue of high-risk vendors of 5G equipment. This toolbox was endorsed by the Commission and the European Council. The criteria in the toolbox offer an operational framework that is useful for assessing the risk profile of suppliers in a coordinated manner across all Member States. At the same time, carrying out this assessment remains a national responsibility. The toolbox was adopted at an early stage of the 5G deployment, but a number of MNOs had already selected their suppliers. 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. In the years to come, legislation on 5G security enacted by Member States based on the toolbox may lead to more convergent approaches towards high-risk 5G vendors. However, as none of the measures put forward are legally binding, the Commission has no power to enforce them. Therefore, there remains a risk that the toolbox in itself cannot guarantee that Member States address network security aspects in a concerted manner.

VIII The Commission has started addressing the issue of foreign subsidies to 5G vendors, with possible security implications. The Commission does not have sufficient information regarding the Member States' treatment of potential substitution costs that could arise if MNOs would need to remove high-risk vendors' equipment from EU networks without a transitional period.

IX We recommend that the Commission should:

- promote the even and timely deployment of 5G networks within the EU;
- foster a concerted approach to 5G security among Member States; and
- monitor Member States' approaches towards 5G security and assess the impact of divergences on the effective functioning of the single market.

Introduction

Nature and importance of 5G

01 The "fifth generation" of telecommunication systems, or 5G, is a new global wireless standard. Compared to the 3G and 4G networks, it offers much greater data capacity and transmission speeds. 5G includes some network elements based on previous generations of mobile and wireless communications technology, but it is not an incremental evolution of these networks. It provides universal ultra-high bandwidth and low latency connectivity for individual users and connected devices.

02 5G will connect more devices than ever before in the “internet of things”. By the end of 2018, there were an estimated 22 billion connected devices in use worldwide. This figure is forecast to increase to around 50 billion by 2030[1], creating a massive web of interconnected devices spanning everything from smartphones to kitchen appliances. The global consumption of data is expected to jump from 12 exabytes of mobile data traffic per month in 2017[2] to over 5 000 exabytes by 2030[3].

03 5G services are essential for a wide range of innovative applications which have the potential to transform many sectors of the EU economy and improve citizens’ daily lives (see ***Figure 1***). A 2017 study carried out for the Commission indicated that the benefits of 5G introduction across four key strategic industrial sectors (automotive, health, transport and energy) may be as high as €113 billion euro per year[4]. The study also anticipated that the implementation of 5G could create 2.3 million jobs in the Member States. A 2021 study estimated that between 2021 and 2025, 5G would add up to €1 trillion to the European gross domestic product (GDP) for the period, with the potential to create or transform up to 20 million jobs across all sectors of the economy[5].

---

1 Statista, Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030.

2 Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017-2022, February 2019.

3 ITU-R, IMT traffic estimates for the years 2020 to 2030.

4 Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, February 2017.

5 Accenture Strategy, The Impact of 5G on the European Economy, February 2021.

Figure 1 – 5G will cover all aspects of our life

Source: European Commission.

Security concerns

04 While 5G has the potential to unleash many opportunities for growth, it comes with certain risks (see ***Annex I*** outlining the main opportunities and risks of 5G). One such risk is that of security threats. Telecommunication systems have always been at risk of cyber-attacks (see ***Annex II***)[6]. Security issues are a particular concern regarding 5G because it offers a larger attack surface than 3G or 4G telecommunication systems due to the nature of its technology and in particular its reliance on software[7].

05 With 5G networks expected to become the backbone of a wide range of services and applications, the availability of those networks will become a major national and EU security challenge. If hackers were to penetrate a 5G network, they could compromise its core functions to disrupt services or seize control of critical infrastructure (for example power grids), which in the EU often has a cross-border dimension. Studies estimate that the economic impact of cybercrime may be as much as €5 000 billion a year worldwide, i.e. over 6 % of global GDP in 2020[8].

---

[6] Review 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper); 2020 Contact Committee Audit Compendium – Cybersecurity; and European Parliamentary Research Service – European Science-Media hub.

[7] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, 9.10.2019. Point 3.4.

[8] World Economic Forum, Wild Wide Web – Consequences of Digital Fragmentation, 2021.

06 Another 5G security challenge is the critical role of a limited number of vendors in building and operating 5G networks. This increases the exposure to potential disruption of supply when there is dependency on a single vendor – particularly if this vendor presents a high degree of risk – such as by being subject to interference from a non-EU country. In 2019, the Network and Information System (NIS) Cooperation Group – composed by representatives of the Member States and of EU bodies – pointed to the risk of "hostile state actors" obtaining an easy entry point to a 5G network either through privileged access, by applying pressure on a vendor or by invoking national legal requirements[9] (see ***Box 1***). It is against this background that the EU started developing initiatives in the area of 5G security.

Box 1

Security concerns in the context of EU-China cooperation on 5G

- In 2015, the EU signed a joint declaration with China on strategic cooperation on 5G, committing to reciprocity and openness in terms of access to 5G networks research funding and market access[10].
- In 2017, China adopted a national intelligence law stipulating that all Chinese organisations and citizens must collaborate in national intelligence, with safeguards on secrecy[11]. In response, in 2018, the USA took actions to limit the operations of several Chinese companies, including Huawei, a key 5G vendor.

In March 2019, the European Parliament also expressed concerns that Chinese 5G vendors might present a security risk for the EU due to the laws of their country of origin.

07 Confidentiality and privacy are also potentially under threat as telecom operators often outsource their data to data centres. There is a risk that this data is stored on 5G vendors' equipment, located in non-EU countries with different levels of legal and data protection than within the EU.

---

[9] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, 9.10.2019.

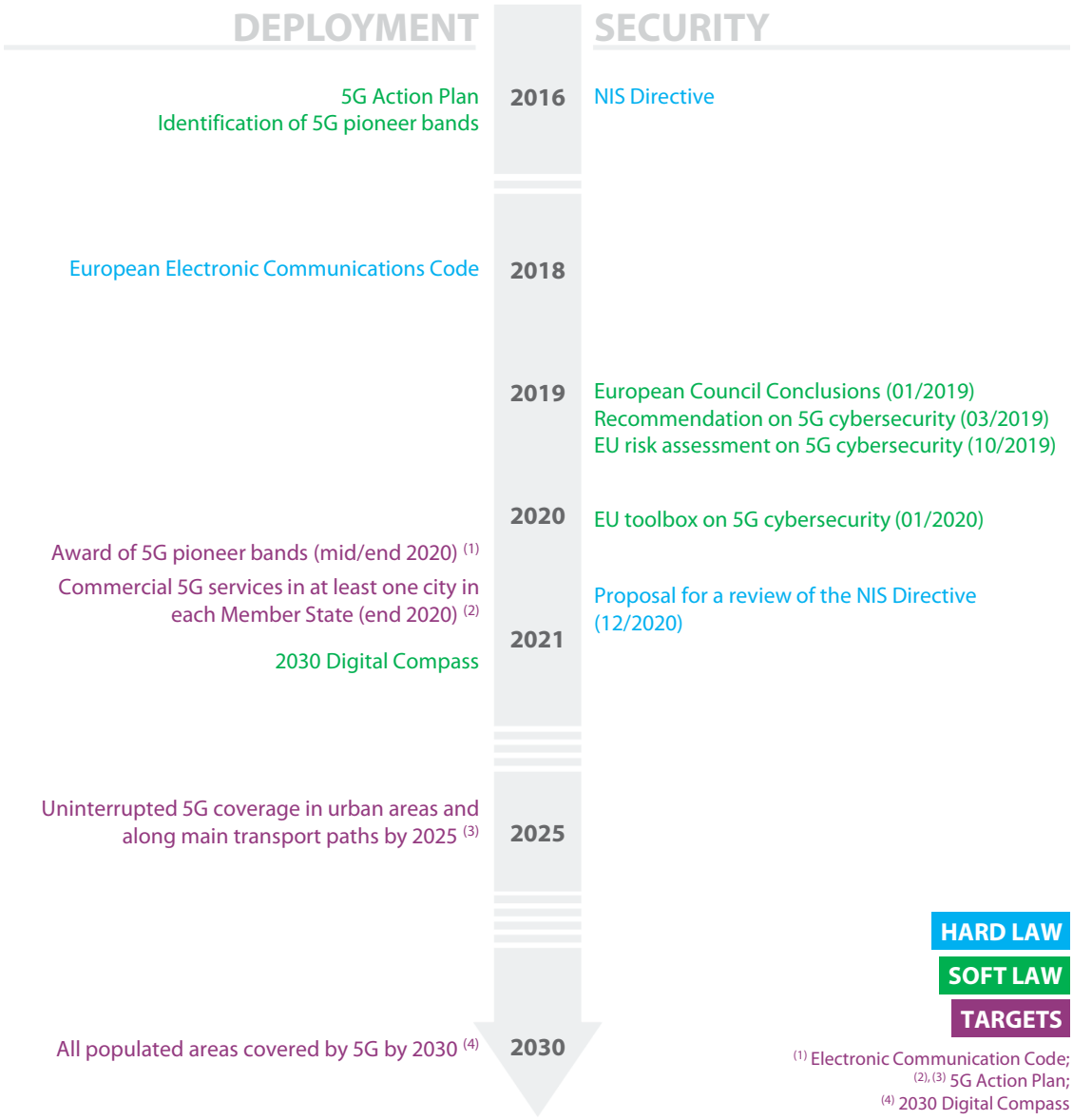
[10] https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5715

[11] European Parliament resolution of 12 March 2019; National Intelligence Law of the People's Republic of China, article 14. See also its translation at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

5G initiatives taken at EU level

08 The policy framework relating to 5G and 5G security is composed of both 'hard law' that is legally binding and enforceable (for example regulations) and non-binding 'soft law' (for example Commission's communications). ***Annex III*** presents the legal and policy framework. ***Figure 2*** shows the main policy documents, along with the key targets.

Figure 2 – Main policy documents and key targets relating to the deployment and security of 5G



Source: ECA.

Roles and responsibilities

09 While mobile network operators (MNOs) are responsible for the secure roll-out of 5G using equipment sourced from technology vendors, and Member States are responsible for national security, 5G network security is an issue of strategic importance for the entire single market and the EU's technological sovereignty[12]. Consequently for the technical and security aspects of 5G networks, the Commission and EU agencies support and coordinate Member States' actions.

10 ***Table 1*** further explains the main roles and responsibilities on 5G networks.

Table 1 – Roles and responsibilities

	Commission and EU agencies	Member States authorities	MNOs & 5G vendors
Allocation and assignment of 5G pioneer bands		✓	
Defining EU 5G policy	✓	✓	
Deployment of 5G networks			✓
Investment and funding	✓	✓	✓
National security		✓	
Security of 5G networks		✓	✓
Support and coordination of Member States' actions	✓		

Source: ECA.

Cost of 5G deployment and related EU financial support

Total cost of 5G deployment across all Member States could reach €400 billion

11 In 2021, the total cost of 5G deployment across all EU Member States until 2025 has been estimated to range between €281 billion and €391 billion, split equally between building new 5G infrastructure and upgrading fixed infrastructure to gigabit speeds[13]. The bulk of these investments need to be financed by the MNOs.

---

[12] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_12

[13] Commission estimate based on data by EIB, Analysis, GSMA and company announcements, and ETNO – European Telecommunications, Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All, March 2021.

In the 2014-2020 period, the EU supported 5G development with over €4 billion

12 During the 2014-2020 period, the EU supported 5G development with over €4 billion, both directly from the EU budget and through the European Investment Bank (EIB) financing. The EU budget funded projects related exclusively to research, while the EIB supported both research and deployment.

13 The EIB has been the biggest provider of EU financing for 5G related projects. As of August 2021, it provided loans for a total of €2.5 billion for nine 5G projects in five Member States[14]. Furthermore, around €1.9 billion was made available from the EU budget for the 2014-2020 period. ***Table 2*** summarises the main sources of EU financial support for 5G.

Table 2 – EU financing for 5G (2014-2020)

EU financing	Amount
EIB	€2.485 billion[1]
European Fund for Strategic Investments (EFSI)	€1 billion[2]
Horizon 2020	€755 million[3]
ERDF	At least €147 million[4]

(1) EIB project list.
(2) EFSI project list.
(3) Horizon 2020 dashboard.
(4) Dataset of projects co-funded by the ERDF during the multi-annual financial framework 2014-2020.

Source: ECA.

14 The EFSI (which is operated by the EIB) supported two projects aiming at reaching a denser cell deployment and supporting standardisation. The total investment cost of these projects was €3.9 billion, including €1 billion financing from EFSI (see ***Annex IV***).

15 Since 2014, the Commission has also directly co-financed, more than 100 5G projects through Horizon 2020 funding and, to a lesser extent, the ERDF. ***Annex V*** presents examples of such projects.

[14] EIB project list.

The Recovery and Resilience Facility will provide additional EU funding for 5G deployment in the coming years

16 The Recovery and Resilience Facility (RRF) will provide a supplementary source of funding for the 5G deployment in the coming years. As of September 2021, 16 Member States were planning to finance 5G deployments through the RRF and 10 had decided not to do so. Information was not yet available from the last Member State.

Audit scope and approach

17 Through this audit we assessed whether the Commission is effectively supporting Member States in:

- achieving the EU's 2025 and 2030 objectives for the deployment and roll-out of their 5G networks; and
- addressing 5G security concerns in a concerted manner.

In both these areas, we also examined the Member States' measures and activities.

18 With "5G security" we refer to cybersecurity and security of hardware/software. We examined both security and implementation of 5G networks, for which 2020 was a key year (see ***Figure 2***). Through our report, we aim to provide insights and recommendations on the timely deployment of secure 5G networks in the EU.

19 Our audit covers the period between 2016 and May 2021. As far as possible, we included further up-to-date information. As part of our audit work we:

- reviewed EU legislation, Commission initiatives and other relevant documentation;
- interviewed representatives of the Commission, the EIB, the Body of European Regulators for Electronic Communications (BEREC), the European Union Agency for Cybersecurity (ENISA), telecom associations, MNOs, 5G vendors, international organisations, experts in the field to gather insights, as well as authorities in Finland, Germany, Poland and Spain . The selection of Member States was based on criteria such as the amount of EU funds dedicated to 5G projects, the status of deployment, and considering a geographical balance;
- surveyed all 27 EU national telecom regulatory authorities to gather a broader perspective on 5G challenges in Member States; and
- reviewed ten EU co-financed projects (EFSI, ERDF and Horizon 2020) relating to 5G, selected for illustrative purposes.

20 We also drew from our recent review of the EU´s response to China´s state-driven investment strategy[15] as well as other reports on, for example, broadband[16], the Digitising European Industry initiative[17] and the EU's cybersecurity policy[18].

[15] Review 03/2020 'The EU´s response to China´s state-driven investment strategy'.

[16] Special report 12/2018 'Broadband in the EU Member States: despite progress, not all the Europe 2020 targets will be met'.

[17] Special report 19/2020 'Digitising European Industry: an ambitious initiative whose success depends on the continued commitment of the EU, governments and businesses'.

[18] Review 02/2019 'Challenges to effective EU cybersecurity policy (Briefing Paper)'.

Observations

Delays in the deployment of 5G networks are putting at risk the achievement of the EU's 2025 and 2030 objectives

21 As regards the timely deployment of 5G networks, we examined whether:

- Member States are on track with 5G deployment;
- the Commission has provided Member States with appropriate support; and
- Member States have removed key obstacles to the swift roll-out of 5G networks.

Member States are lagging behind with 5G implementation

The Commission set deadlines for the deployment of 5G networks in its 2016 5G Action Plan

22 In its 2016 5G Action Plan, the Commission proposed deadlines regarding the deployment of 5G networks in the EU: Member States were to have launched early 5G networks by the end of 2018, fully commercial 5G services in at least one major city by the end of 2020, and ensured uninterrupted 5G coverage in urban areas and along main transport paths by 2025.

23 In March 2021, the Commission added a further deadline for the 5G coverage of all populated areas by 2030[19].

23 Member States launched 5G commercial services before end 2020

24 By the end of 2020, 23 Member States had achieved the objective of at least one major city having access to 5G services. Only Cyprus, Lithuania, Malta and Portugal failed to meet this objective. As of the end October 2021, only Lithuania and Portugal still had no 5G services in any of their cities.

---

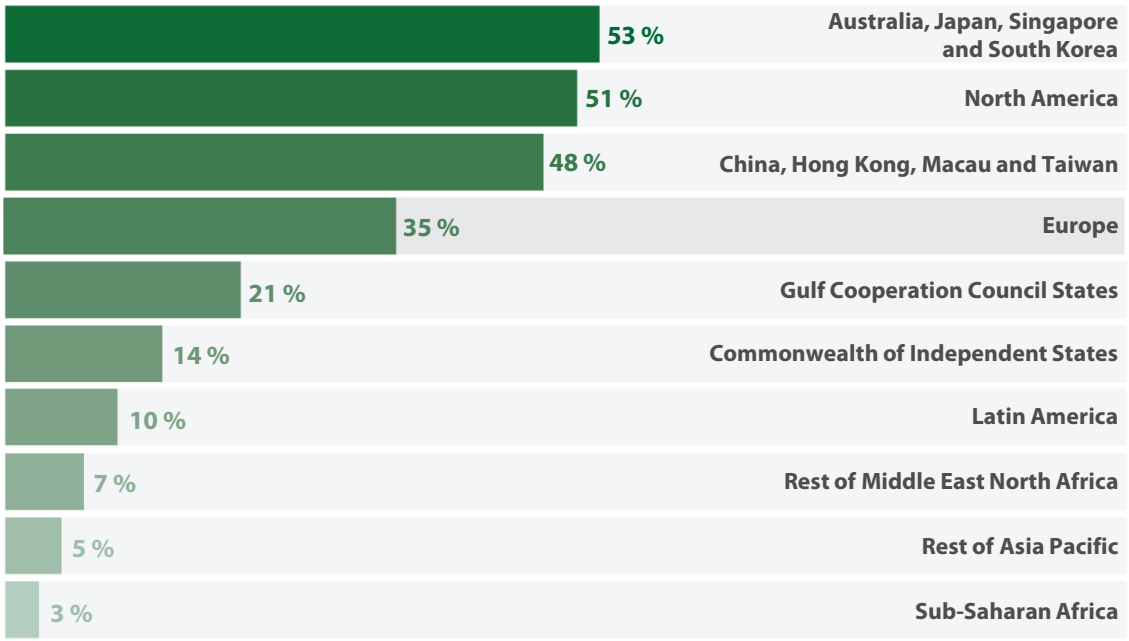
[19] European Commission, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.

There is a risk that most Member States will miss the 2025 and 2030 deadline

25 According to a recent Commission study, only 11 Member States are likely to achieve an uninterrupted 5G coverage in all their urban areas and along major terrestrial transport paths by 2025[20]. For the remaining 16 Member States, the Commission considers that the probability of achieving this objective is either medium (Austria, Czechia, Estonia, Germany, Ireland, Poland, Lithuania and Slovenia) or low (Belgium, Bulgaria, Croatia, Cyprus and Greece).

26 In 2021, the industry organisation Global System for Mobile Communications Association (GSMA) noted that 5G deployment is progressing at different pace in the EU compared to other parts of the worlds. For example, it estimated that 51 % of all mobile connection in North America will be based on 5G by 2025, but in Europe (which also includes non-EU countries) this is only expected to be 35 % (see ***Figure 3***).

Figure 3 – 5G connections as share of total mobile connections by 2025



Source: GSMA. The Mobile Economy 2021.

27 At the current pace of deployment, there is a high risk that the 2025 deadline – and therefore also the 2030 one for the coverage of all populated areas – will be missed by a majority of Member States. Against this background we examined whether the Commission has effectively supported Member States to achieve the EU's 2025 and 2030 5G objectives for the deployment and roll-out of their 5G networks.

[20] Study on National Broadband Plans in the EU-27.

Some shortcomings in the Commission's support for Member States

The Commission did not define the expected quality of service of 5G networks

28 So far, the Commission, has not defined the expected quality of service of 5G networks, such as in terms of minimum speed and maximum latency. Furthermore, the 2016 Action Plan asked Member States to launch "fully commercial" 5G services in Europe by the end of 2020, but without defining these quality related concepts.

29 The lack of clarity on the expected quality of service creates the risk that these terms are interpreted differently by Member States. We noted examples of divergent approaches in 5G deployment between Member States (see ***Box 2***).

Box 2

Examples of divergent approaches in 5G deployment

Speed and latency are two key aspects of the performance of services using 5G. For example, 5G remote surgery or industrial automation require very high speed and low latency. However, so far, only two Member States (Germany and Greece) have defined minimum speed and maximum latency requirements[21].

The need to have "at least one major city having access to 5G services by the end of 2020" has been interpreted differently by Member States. This leads to a situation where a city classified as "having access to 5G services" can range from having only few streets covered – such as in Luxembourg – to having almost its whole territory covered, such as in Helsinki. ***Annex VI*** provides, for selected cities, examples of coverage.

30 If it persists, this situation could lead to inequalities in the access and quality of 5G services in the EU ("digital divide"): people in part of the EU would have better access and quality of service to 5G than others. This digital divide could also affect the potential of economic development as 5G can revolutionize sectors such as health care, education and the workforce only if accompanied by a sufficient 5G performance.

[21] 5G Observatory Quarterly Report 12, Up to June 2021.

31 Clarity on the expected performance of 5G networks is also needed in the light of the Commission's initiative to impose an increased transparency regarding the quality of service provided by the MNOs for roaming, for which the Commission has recently made a legislative proposal[22].

The Commission's quarterly reporting on 5G roll-out not always reliable

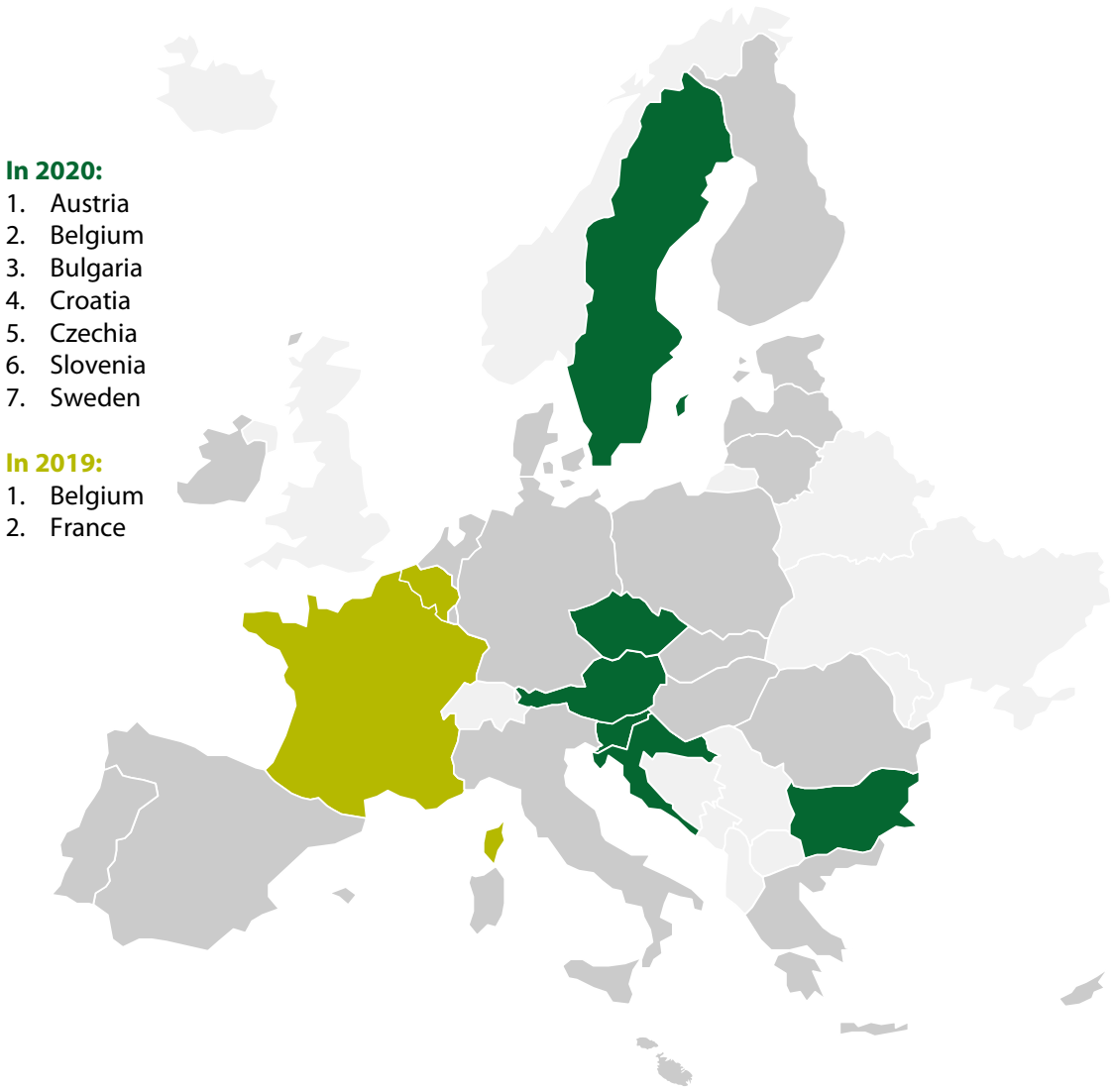
32 The Commission monitors the level of 5G deployment in the Member States through the 5G Observatory. This observatory provides information on 5G deployments and on Member States' 5G strategies on a quarterly basis. We found, however, that for two of the four countries we reviewed, the information contained in these reports was not always reliable. For example, the quarterly report 10, presenting the information up to end December 2020 , put forward a much lower number of municipalities with 5G in Finland than the actual figure (40 instead of 70) and provided no information on the fact that 5G spectrum auctions had been postponed in Poland (see paragraph ***42***).

The Commission only recently made use of the European Semester process to monitor Member States' progress in deploying 5G networks

33 We found that over the last two years the Commission has made greater use of the European Semester process to encourage Member States' progress in deploying 5G networks. The country specific recommendations directly relevant to 5G increased from being addressed to two Member States in 2019, to seven Member States in 2020 (see ***Figure 4***).

[22] European Commission, Proposal for a Regulation on roaming on public mobile communications networks within the Union (recast), COM(2021) 85 final of 24.2.2021.

Figure 4 – Country specific recommendations on 5G



Source: ECA, based on country specific recommendations.

Member States still need to remove key obstacles to the swift roll-out of 5G networks

34 In order to reach the EU's 2025 and 2030 5G deployment objectives, Member States must achieve three major building blocks: strategic, by ensuring that their national 5G strategies or national broadband plans (NBPs) reflect these objectives[23]; legislative, with the transposition of the 2018 European Electronic Communications Code (EECC)[24]; and business-oriented, with the assignment of the spectrum[25]. ***Table 3*** provides an overview of the Member States' progress on these three elements.

[23] Commission' Study on National Broadband Plans in the EU-27.

[24] Directive (EU) 2018/1972 establishing the European Electronic Communications Code.

[25] European Commission's Communication, Secure 5G deployment in the EU – Implementing the EU Toolbox, COM(2020) 50 final.

Table 3 – State of play on building blocks towards the 2025 objectives

Member State	NBP in line with the 2025 objectives	EECC transposition	5G pioneer bands (August 2021)			Likelihood of achieving the objective
			700 MHz	3.6 GHz	26 GHz	
Belgium				Provisional use		low
Bulgaria		✓		✓		low
Czechia	✓	✓	✓	✓		medium
Denmark		✓	✓	✓	✓	high
Germany	✓	✓	✓	✓	✓	medium
Estonia						medium
Ireland				✓		medium
Greece	✓	✓	✓	✓	✓	low
Spain	✓		✓	✓		high
France	✓	✓	✓	✓		high
Croatia			✓	✓	✓	low
Italy			✓	✓	✓	high
Cyprus	✓		✓	✓		low
Lithuania	✓					medium
Latvia				✓		high
Luxembourg			✓	✓		high
Hungary	✓	✓	✓	✓		high
Malta		✓				medium
Netherland	✓		✓			medium
Austria	✓	✓	✓	✓		medium
Poland	✓					medium
Portugal				Provisional use		medium-high
Romania						high
Slovenia	✓		✓	✓	✓	medium
Slovakia			✓			high
Finland	✓	✓	✓	✓	✓	high
Sweden	✓		✓	✓		high

Source: Commission' Study on National Broadband Plans in the EU-27, 5G Observatory and RSPG.

Few Member States have included the 2025 and 2030 deployment objectives in their national 5G strategies

35 Member States set out their 5G policy through dedicated national 5G strategies or by updating their existing NBPs. The 2021 Commission study on NBPs[26] notes that only 14 Member States have included the EU objective of having "an uninterrupted 5G coverage for all urban areas and major terrestrial transport paths by 2025" in their national 5G strategies or update of NBPs (see ***Table 3***). Such inclusion is key to support the successful implementation of the policy.

Most Member States failed to transpose the EECC Directive by end 2020

36 The EECC – a directive laying down tasks of national regulatory and other competent authorities and setting deadlines for the assignment of 5G pioneer bands – should have been transposed by Member States by 21 December 2020. By the end of February 2021, only three Member States (Finland, Greece and Hungary) had declared having adopted all necessary measures for transposing the Directive. Consequently, the Commission opened infringement procedures against the remaining 24 Member States[27].

37 As of the end of November 2021, 23 infringement procedures are still ongoing. While for six Member States the Commission expects to close the infringement procedure soon (Austria, Bulgaria, Czechia, France, Germany and Malta), for the other 17 Member States the Commission may need to refer them to the Court of Justice[28] (see ***Table 3***).

The assignment of 5G pioneer bands is lagging behind

38 In 2016, the Commission and Member States identified three pioneer bands to be used for 5G services:

- the 700 MHz band spectrum makes it easier for wireless signals to penetrate buildings and allows operators to provide wider coverage (hundreds of square km). However, the speed and latency of the 5G network is only a step up from 4G (from 150 to 250 megabits per second);

[26] Study on National Broadband Plans in the EU-27.

[27] Commission press release IP/21/206 of 4.2.2021.

[28] Commission press release IP/21/4612 of 23.9.2021.

- the mid-band spectrum at 3.6 GHz, which can carry significant amounts of data (up to 900 megabits per second) over significant distances (several km radius); and
- the high-band spectrum at 26 GHz, delivering fast speeds between 1 to 3 gigabits per second over short distances (i.e. less than 2 km), but with more sensitivity to interference.

39 Member States were supposed to make the low-band spectrum available for use by 30 June 2020[29], with the mid and high-band spectrums to follow by 31 December 2020[30]. However, by end 2020, Member States had assigned less than 40 % of the total available pioneer bands (see ***Table 4***):

- the 700 MHz band was assigned in 13 Member States;
- the 3.6 GHz band was assigned in 17 Member States (including two Member States which had granted provisional use); and
- the 26 GHz band was assigned in four Member States.

By the end of October 2021, the assignment rate had increased to 53 %[31].

[29] Decision (EU) 2017/899 on the use of the 470-790 MHz frequency band.

[30] Directive (EU) 2018/1972 establishing the European Electronic Communications Code.

[31] 5G Observatory and RSPG.

Table 4 – State of play on the assignment of 5G pioneer bands, December 2020

Member State	700 MHZ	3.6 GHZ	26 GHZ
Belgium		Provisional use	
Bulgaria			
Czechia	✓	✓	
Denmark	✓		
Germany	✓	✓	✓
Estonia		-	
Ireland		✓	
Greece	✓	✓	✓
Spain		✓	
France	✓	✓	
Croatia			
Italy		✓	✓
Cyprus	✓	✓	
Latvia		✓	
Lithuania			
Luxembourg	✓	✓	
Hungary	✓	✓	
Malta			
Netherland	✓		
Austria	✓	✓	
Poland			
Portugal		Provisional use	
Romania			
Slovenia			
Slovakia	✓	✓	
Finland	✓	✓	✓
Sweden	✓	✓	

Source: 5G Observatory and RSPG.

Delays in assigning the pioneer bands are attributable to a range of reasons

40 We found that delays in assigning the 26 GHz band are mainly due to a weak demand by MNOs. In Spain for example, a total of 1.5 GHz of the 26 GHz band is available for 5G use. However, it has not yet been assigned to operators because there is no demand for it, according to a public consultation finalised in July 2019. A new public consultation is planned by the end of 2021, with a view to auctioning the band in the second quarter of 2022. Also MNOs in Finland noted that there is not much interest or a business case yet for the 26 GHz band.

41 Cross-border coordination issues with non-EU countries along the eastern borders (Belarus, Russia, and Ukraine) have also contributed to delays in the assignment of 5G spectrum. These non-EU countries are, under the current international agreements, using the 700 MHz band for TV broadcasting and the 3.6 GHz band for military satellites services. This issue mainly concerns the Baltic countries (Estonia, Latvia, and Lithuania) and Poland. According to the Commission, there has been some progress with Ukraine and Belarus, which should release the 700 MHz band by the end of 2022. Bilateral talks with Russia have not yet progressed. In view of this situation, Estonia and Poland have requested a derogation from the deadlines for the assignment of the 700 MHz band until mid-2022.

42 In addition, in Poland and Spain, 5G spectrum auctions were postponed during the COVID-19 pandemic (see ***Box 3***).

Box 3

Examples of delays caused by COVID-19 in the assignment of 5G spectrum

- In March 2020, Poland announced an auction for the 3.6 GHz band, which was to be awarded by 30 June 2020. Following the pandemic outbreak, Polish authorities decided to suspend all administrative proceedings for the duration of the pandemic. As of September 2021, the process for auctioning this band was still not completed.

- In Spain, the auction for the 700 MHz band, was initially planned for March 2020. However, according to the Spanish authorities, the COVID-19 pandemic delayed the release of this band used for digital television. Subsequently, the auction was postponed until May 2020 and then to the first quarter of 2021. Following an amendment of the Spanish legislation in April 2021 to align the duration of licences with the EECC, the auction was rescheduled for the summer of 2021 and the 700 MHz band was finally awarded in July 2021.

43 One further reason delaying the assignment of the 5G pioneer bands is Member States' different approaches on 5G security and the delays in adopting their 5G security laws, which generates business uncertainty (see paragraphs ***74*** and ***75***):

- In Spain, the pioneer band auction rules included a general clause stating that the holders of public concessions must comply with all obligations for the security of 5G networks established at any time in the future by the European or Spanish regulations. The Spanish MNO we interviewed considered that this clause obliged it to make decisions about strategies and purchases under conditions of uncertainty. It also pointed out that the national authorities were unwilling to clarify certain key conditions, such as the possibility of compensation if the future legislation, planned to be adopted by the end of 2022, required them to replace their equipment.

- In Poland, one of the reasons given for postponing the assignment of 5G spectrum was the need to wait for a law clarifying the security requirements for 5G networks.

Further efforts are necessary to address security issues in 5G deployment

44 As regards the security aspects of 5G, we examined whether:

- the Commission has taken the necessary steps to promote a sound design of the security framework, and provided adequate support to Member States; and

- Member States are implementing secure 5G networks in a concerted manner, adopting the mitigating measures included in the EU toolbox on 5G cybersecurity (toolbox) and updating their legislation.

The Commission reacted swiftly when 5G security became a major concern at EU level

45 The 2016 5G Action Plan does not include any security considerations. The security of 5G networks and an over reliance on vendors from third countries, and in particular China, was identified as a critical issue in March 2019. The European Parliament, in its resolution of 12 March 2019[32], raised concerns about non-EU 5G vendors that might present a security risk for the EU due to the laws of their countries of origin. The same day, the Commission in its strategic outlook on the EU-China relationship highlighted that a common EU approach to the security of 5G networks is needed to safeguard against potential serious security implications for critical digital

[32] European Parliament resolution of 12 March 2019 (2019/2575(RSP)).

infrastructure[33]. The European Council in its conclusions of 21 and 22 March 2019, asked the Commission to issue a recommendation on a concerted approach to the security of 5G networks[34].

46 A few days later, the Commission issued such a recommendation featuring a set of measures both at national (for example risk assessment on 5G) and EU level (for example coordinated risk assessment), aiming at ensuring a high level of cybersecurity of 5G networks across the EU[35].

47 Almost all Member States had completed their national risk assessments by the deadline of July 2019[36]. In October 2019, the NIS Cooperation Group issued a report on the EU's coordinated risk assessment of the cybersecurity of 5G networks, and the "EU Toolbox on 5G cybersecurity"[37] in January 2020 (see ***Annex VII***). It was swiftly endorsed by the Commission and the European Council[38].

The 2020 EU toolbox on 5G cybersecurity for the first time established measures to deal with security threats at EU level, without prescriptiveness

Approaching the security of 5G networks as a national security competence limits the Commission's scope for action

48 The EU treaties[39] determine the scope for action to tackle challenges such as those relating to the deployment of secure 5G networks at EU level. This scope is wide and leaves a margin of interpretation to the Commission and Member States (see ***Box 4***).

---

[33] JOIN(2019) 5 final of 12.3.2019. EU-China – A strategic outlook.

[34] European Council conclusions of 21 and 22 March 2019.

[35] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks.

[36] Press release of 19 July 2019.

[37] Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures. NIS Cooperation Group, 01/2020.

[38] European Commission's Communication, Secure 5G deployment in the EU – Implementing the EU Toolbox, COM(2020) 50 final; and European Council conclusions of 1 and 2 October 2020 (EUCO 13/20).

[39] Treaty on the Functioning of the European Union.

Box 4

EU competences related to 5G networks: A shared competence or a matter of national security?

In principle, 5G networks fall within the scope of the EU's single market competence (a shared competence), both as a service (the provisions of a service by MNOs) and as a good (the 5G equipment itself, purchased by MNOs to build their 5G networks). As a shared competence, the EU (the Commission and other EU institutions) may adopt legally binding measures (legislation) to ensure the establishment of its single market and promote its proper functioning. The security of 5G networks could also be considered more broadly as relating to the EU's area of freedom, security and justice. In this sense, security can be understood as a general term relating to the prevention and combatting of crime, which makes it another shared competence for which the EU may adopt legally binding measures.

By contrast, a more narrow interpretation of security would be to limit it to threats to the national security of Member States. As an exclusive national competence, this limits the EU to only being able to undertake supporting actions to help the national efforts of Member States to ensure the security of their 5G networks.

49 The security of 5G networks cuts across national and EU competences and touches upon national security. The Commission approached the security of 5G networks in the sense of threats to the national security and therefore opted for "soft law" measures. This implies that the EU cannot adopt legally binding measures that would compel the Member States to apply uniform risk-mitigating measures or implement enforceable requirements. Instead, the Commission can issue non-binding recommendations and communications, help to disseminate best practice and coordinate the national actions of Member States. Yet, a different approach is possible. Such an example is the NIS Directive[40], which is an EU law dealing with the security of network and information systems across the Union. This law was proposed

[40] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

by the Commission and adopted under the 'single market' legal base, although, to a large extent, cybersecurity is a national prerogative[41].

The EU toolbox on 5G cybersecurity was adopted at an early stage of deployment, but some MNOs had already selected their vendors

50 In January 2020, the NIS Cooperation Group adopted an EU toolbox on 5G cybersecurity, which specifies a number of strategic, technical and support measures to deal with 5G security networks threats and identifies the relevant actors for each of these measures. This toolbox, endorsed by the Commission and the European Council, was adopted only nine months after the European Parliament and the Council had raised their concerns about 5G security for the first time. More recently, the EU toolbox on 5G cybersecurity has been mentioned in the new European Strategy to boost smart, clean and secure links in digital systems across the world, as a tool to guide investments in digital infrastructure[42]. The soft law approach put in place by the Commission contributed to putting into motion rapidly measures to deal with security threats also at EU level and to facilitate Member States' cooperation on this cross-border topic. For comparison, the NIS directive necessitated more than three years from the Commission proposal[43] to its adoption[44], and the EECC directive over two years[45]. Even more time was necessary for the directives to be transposed into the national legal systems of the Member States (see also paragraph ***36*** and ***37***).

51 The EU toolbox on 5G cybersecurity was adopted four years after the 5G policy had been presented in the 5G Action Plan, and the same year as intermediate deployment milestones set under this 5G Action Plan would have had to be achieved. In this context, representatives of Member State ministries, National Regulatory Authorities and MNOs interviewed for this audit considered that the measures on security aspects of 5G started too late.

---

41 Review 02/2019 'Challenges to effective EU cybersecurity policy (Briefing Paper)', paragraph 36.

42 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank – The Global Gateway. JOIN(2021) 30 final, 1.12.2021.

43 COM(2013) 48 final of 7.2.2013.

44 Directive (EU) 2016/1148.

45 COM(2016) 590 final/2 of 12.10.2016 and Directive (EU) 2018/1972 establishing the European Electronic Communications Code.

52 At the same time, the toolbox was published when 5G deployments and plans were still in an early stage in most Member States. Most of the contracts between suppliers and operators for 5G equipment were concluded in 2020 and 2021. However, according to European Telecommunications Network Operators' Association (ETNO), a number of MNOs had already selected their vendors when the EU toolbox on 5G cybersecurity became available.

The EU toolbox on 5G cybersecurity provided a framework for assessing the risk profile of suppliers, but shortcomings remained

Some Member States and national authorities consider part of the criteria used to classify vendors as high-risk as not sufficiently clear

53 A key feature of the EU toolbox on 5G cybersecurity is the need for Member States to assess vendors and to apply, for key assets defined as critical, restrictions to vendors classified as high-risk. Member States should make this assessment on the basis of a non-exhaustive list of criteria taken from the EU's coordinated risk assessment. Such criteria are for example:

- the likelihood of a vendor being subject to interference from a non-EU country; for example through the existence of a strong link between the vendor and a government of a non-EU country; or through the non-EU country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the non-EU country;
- the vendor's ability to assure supply; and
- the overall quality of the vendors' products and cybersecurity practices.

54 The toolbox has been developed to avoid fragmentation and promote consistency in the internal market. The criteria in the toolbox offer an operational framework that is useful for assessing the risk profile of suppliers in a coordinated manner across all Member States. It also allowed the Commission to react swiftly to emerging 5G security concerns, together with Member States. At the same time, it remains the national authorities' responsibility to apply these criteria when assessing the risks related to specific suppliers. By October 2021, taking account of this framework, 13 Member States have enacted or amended legislation on 5G security (see paragraph ***75*** and ***Figure 6***).

55 However, the representatives of two out of the four Member State ministries whom we interviewed for this audit considered that some of these criteria for classifying 5G vendors are open to interpretation and would need to be further clarified. They also called for the Commission to provide additional support and guidance regarding the classification of high-risk vendors. Member State representatives interviewed also indicated that this situation created a risk of Member States applying divergent approaches on high-risk vendors (see also paragraphs ***74*** and ***75***, and ***Box 5***). Eleven of the national regulatory authorities surveyed, which have different degrees of involvement in 5G security, voiced similar concerns.

5G vendors' country of origin affects the assessment of security risks

56 5G vendors vary in terms of their corporate characteristics, and are from countries with different ties to the EU. ***Figure 5*** presents some commonalities and differences between the main 5G vendors and their countries of origin, particularly in areas referred to in the toolbox as likely to influence the assessment of their risk profile (see paragraph ***53***).

Figure 5 – Commonalities and differences between 5G vendors and their countries of origin

Source: ECA, based on WTO members; OECD members; OECD FDI Restrictiveness Index; World Bank, Worldwide Governance Indicators Dataset, 2019; WEF Global Competitiveness Dataset, Ranking in 2018; Adequacy decisions; Statista, Who is leading the 5G patent race?; Ericsson company data; Nokia company data; Qualcomm company data; Sharp company data; LG company data; Samsung company data; Huawei company data; and ZTE company data. Exchange rates as of 31.12.2020.

57 One risk factor is the degree to which a vendor's country of origin complies with the EU's core political and economic values. Country-specific related factors such as the rule of law, judicial independence, openness to foreign investments and the existence of data protection agreements can be taken as a measure of a company's legal protection from government interference and the protection it can pass on to its customers.

58 While vendors based in EU Member States are bound to comply with the EU standards and legal requirements, this is not the case for six of the main vendors located in non-EU countries which operate within the framework of third country legislations (see ***Figure 5***). Such legislations can differ considerably from the EU standards, for example in terms of data protection accorded to citizens, effectiveness of such protection, or more generally on how judicial independence is ensured by legislative and/or democratic checks and balances. When it comes to judicial independence, the USA and Japan score higher than the other non-EU countries of origin of 5G vendors, while for the rule of law rating, it is South Korea that scores the best among the non-EU countries.

59 5G networks are pre-dominantly software-run. The fact that some vendors operate within the framework of non-EU legislation may be of particular concern where the software control centres are also outside the EU, potentially making EU users subject to non-EU legislation.

60 The Commission has started addressing these concerns, considering that any business providing services to EU citizens should respect the EU's rules and values[46]. It has started dialogues with several countries to secure strong privacy protections for personal data[47]. ***Figure 5*** also shows that the Commission has already recognised the adequacy of Japan's (and, in the past, the US) data protection regimes. It should be noted, though, that adequacy decisions can be challenged and are subject to strict judicial scrutiny. As an example, in 2015 the European Court of Justice struck down the then applicable legal instrument for data exchange with the United States, the Safe Harbour arrangement[48], and later in 2020, it ruled that the Privacy Shield – which had

---

[46] European Commission's Communication, Shaping Europe's digital future, COM(2020) 67 final.

[47] EU-China – A strategic outlook.

[48] Judgment in Case C-362/14 and https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

replaced the Safe Harbour Agreement – did not provide adequate protections to EU citizens[49]. There is thus currently no adequacy decision for the United States. More generally, and beyond the existence of a data protection regime, it is important to take into account the broader legal and institutional framework, including for instance respect for rule of law and the way judicial independence is ensured.

61 ***Figure 5*** also shows a significant variability between the 5G vendors in terms of share of 5G patents, revenue and headcount. This affects the resources at their disposal, which in return may affect their resilience and ability to ensure continued supply. For example, Samsung and Huawei are the vendors which have the highest share of 5G patents and generate the highest revenues as corporations and have the highest number of employees overall.

62 The likelihood of a vendor being subject to interference from the government of a non-EU country is another important factor defined in the toolbox as determining a vendor's risk profile. In this context, ownership plays an important role, as owners with a large number of shares may be able to exercise pressure or influence management decisions. Furthermore, companies under private or state ownership are deemed less open to public scrutiny in terms of audits and accountability, compared to public companies which are subject to stringent disclosure requirements throughout the year for the benefit of general investors and regulators. Most 5G vendors are publicly listed on a stock exchange, either in their country of origin or abroad, whereas the Chinese vendors are harder to classify and are generally perceived as being closely linked to the Chinese government[50].

The Member States found the Commission's and ENISA's support useful when implementing the EU toolbox on 5G cybersecurity

63 The Commission provided support to Member States by exchanging best practices on some key measures of the EU toolbox on 5G cybersecurity, including on high-risk vendors. This support, often provided in the context of the NIS Cooperation Group, was complemented by specific ENISA activities such as organising webinars or providing guidance on:

---

[49] Judgment in Case C-311/18 and https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

[50] https://www.europarl.europa.eu/doceo/document/E-9-2020-004305_EN.html and https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

- the implementation of the toolbox with a focus on the technical measures; and
- best practices on network security, in particular on:
  - the 5G Threat Landscapes[51];
  - the preparation of national 5G risk assessments; and
  - security measures under the EECC[52], including dedicated guidelines on 5G security[53].

64 The Commission also tasked ENISA with preparing the EU's cybersecurity certification scheme for 5G networks that should help with addressing risks related to technical vulnerabilities of the networks and further enhance cybersecurity[54]. While this certification could contribute to improving security, it cannot prevent threats from being embedded in the systems through software updates.

65 All the representatives of Member State authorities that we interviewed for this audit stressed the usefulness of the Commission's and ENISA's support to implement the EU toolbox on 5G security. Moreover, most of the national telecom regulatory authorities (15 out of 21) stated that the Commission and/or ENISA have supported national authorities in exchanging best practice for implementing the key strategic measures.

EU toolbox on 5G cybersecurity was adopted too late to have been taken into account for EU co-funded projects during the 2014-2020 period

66 One of the objectives of the EU toolbox on 5G cybersecurity is to ensure that EU co-funded 5G projects take cybersecurity risks into account. However, the toolbox was adopted only in January 2020. As all the projects we reviewed for this audit had been selected before the EU toolbox on 5G cybersecurity was adopted, they could not have been expected to have followed the recommended approach on cybersecurity, including towards high-risk vendors. For example, in our sample, we identified one Horizon 2020 and two ERDF projects in Spain using Chinese 5G equipment which was subsequently banned in Sweden (see paragraph ***15***).

---

[51] ENISA, Threat Landscape for 5G Networks, 14.12.2020.

[52] ENISA, Guideline on Security Measures under the EECC, 10.12.2020.

[53] ENISA, 5G supplement to the Guidelines on Security Measures under the EECC, 7.7.2021.

[54] Press release of 3 February 2021.

67 For the 2021-2027 period, the Commission intends to promote a coherent approach on 5G security for EU co-funded projects by ensuring that compliance with the toolbox is a condition for EU funding. This will however vary depending on the implementation mode:

- Programmes directly managed by the Commission (for example the 2021-2027 Horizon Europe) will allow the exclusion of vendors subject to interference from the government of a non-EU country. This is likely to ensure that EU-funded projects take account of cybersecurity risks and to prevent situations where a vendor receiving EU co-financing in one Member State is considered as high-risk and excluded in another;

- For programmes implemented under shared management, the legislation does not contain requirements about cybersecurity risks. Therefore, the Commission envisages promoting the inclusion of a reference to the toolbox in the Member States' partnership agreements as a way allowing ERDF funding for 5G related projects to take account of cybersecurity risks; and

- For the Invest-EU (the programme replacing EFSI)[55] and the RRF, the Commission plans to encourage the responsible bodies to refer to the EU toolbox in the funding agreements.

Member States do not yet address security aspects in a concerted manner when deploying 5G networks

Information on how Member States approach security matters is insufficient

68 The Commission tracks and reports on the progress of implementation of the EU toolbox on 5G cybersecurity through the NIS Cooperation Group, bilateral talks with Member States and indirectly through the media. The first results of this monitoring were published in July 2020[56]. In December 2020, the Commission also published a report on the impact of its Recommendation on the Cybersecurity of 5G networks[57]. As of September 2021, no future reporting is planned.

---

[55] Regulation (EU) 2021/523 establishing the InvestEU Programme.

[56] Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, July 2020.

[57] Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final of 16.12.2020.

69 However, the above-mentioned reports lack a common set of key performance indicators and do not present a comparable set of detailed information on how Member States are approaching 5G security concerns.

70 There is furthermore little publicly available information on how Member States approach high-risk vendors i.e. their identification and whether vendors are being excluded from providing their 5G equipment, and even that is contradictory and incomplete. For example:

- In its July 2020 report on Member States' Progress in implementing the toolbox (see paragraph ***68***), the Commission states that around half of the Member States (14 out of 27) had assessed the risk profile of vendors and applied restrictions for vendors considered to be high-risk.
- In a December 2020 report[58], BEREC stated that only nine Member States had put in place such restrictions, and that seven of the remaining 18 Member States did not intend to implement such restrictions in the future.

71 Even when Member States have adopted legislation addressing the security of 5G networks (see also paragraph ***75***) these still do not clarify the Member States' approach towards high-risk vendors. Any concrete decisions are likely to be taken only through implementing acts or non-public administrative or commercial decisions.

72 According to the stakeholders and decision makers we interviewed (for example at the European Parliament), non-public information (for example through Commission or NIS Group reports) on the Member States' approach towards high-risk vendors is also scarce, and these entities have to rely on media and unofficial sources.

73 Despite the cross-border nature of the 5G security concerns, there is overall little public information available on how Member States approach security matters, in particular the issue of high-risk vendors. This hampers knowledge sharing between Member States and the possibility to apply concerted measures. It also limits the possibility for the Commission to propose improvements to the security of 5G networks.

---

[58] BEREC, Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience), BoR 20 (227), 10.12.2020.

There are indications that some Member States follow divergent approaches towards 5G vendors

74 National authorities have a wide margin of discretion when implementing key measures on 5G security (see paragraphs ***48*** and ***49***). The toolbox takes into account national competences and relevant country-specific factors (threat assessment from national security services, timeframe for deploying 5G, presence of suppliers, cybersecurity capabilities). So far, Member States have applied divergent approaches regarding the use of equipment from specific vendors or the scope of restrictions on high-risk vendors (see examples of four Member States in ***Box 5***).

Box 5

Examples of Member States' divergent approaches towards Chinese 5G vendors

Framework in place and restrictions applied[(1)]

In October 2020, the Swedish national regulatory telecom authority (PTS) imposed the following conditions for participation in the auction of 5G spectrum:

— new installations and implementation of central functions for the radio use in the frequency bands must not use products from Chinese vendors; and

— any existing infrastructure from such vendors must be phased out by 1 January 2025 at the latest.

Framework in place, but not yet applied[(2), (3), (4)]

In Germany, the IT security act 2.0 of May 2021 provides for mandatory certification of critical components before their use can be authorised. The German MNOs that we interviewed would prefer a single European certification procedure under the auspices of ENISA, to serve as a European "one-stop shop", instead of having to go through a potential multitude of national certifications. The act also allows the Federal Ministry of the Interior to prohibit the use of critical components, in case they could pose a threat to national security.

In Austria, the updated telecom law adopted at the end of October 2021 allows the competent minister to classify vendors as high-risk and apply restrictions or exclude them from the market. Publicly available information from October 2021 indicates that the country is on course to expand its 5G network, using the Chinese supplier Huawei.

No framework in place[5], [6]

As of September 2021, Hungary has not restricted any 5G vendor, and is not likely to do so in the near future. Hungary has also officially declined to join the international 5G Clean Network Program, promoted by the USA, which aims to limit the presence of Chinese vendors in 5G core networks.

(1) Decision 18-8496 of 20.10.2020 on the terms for the auction for frequency bands 3.5 GHz and 2.3 GHz.

(2) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

(3) Austria Telecommunication law.

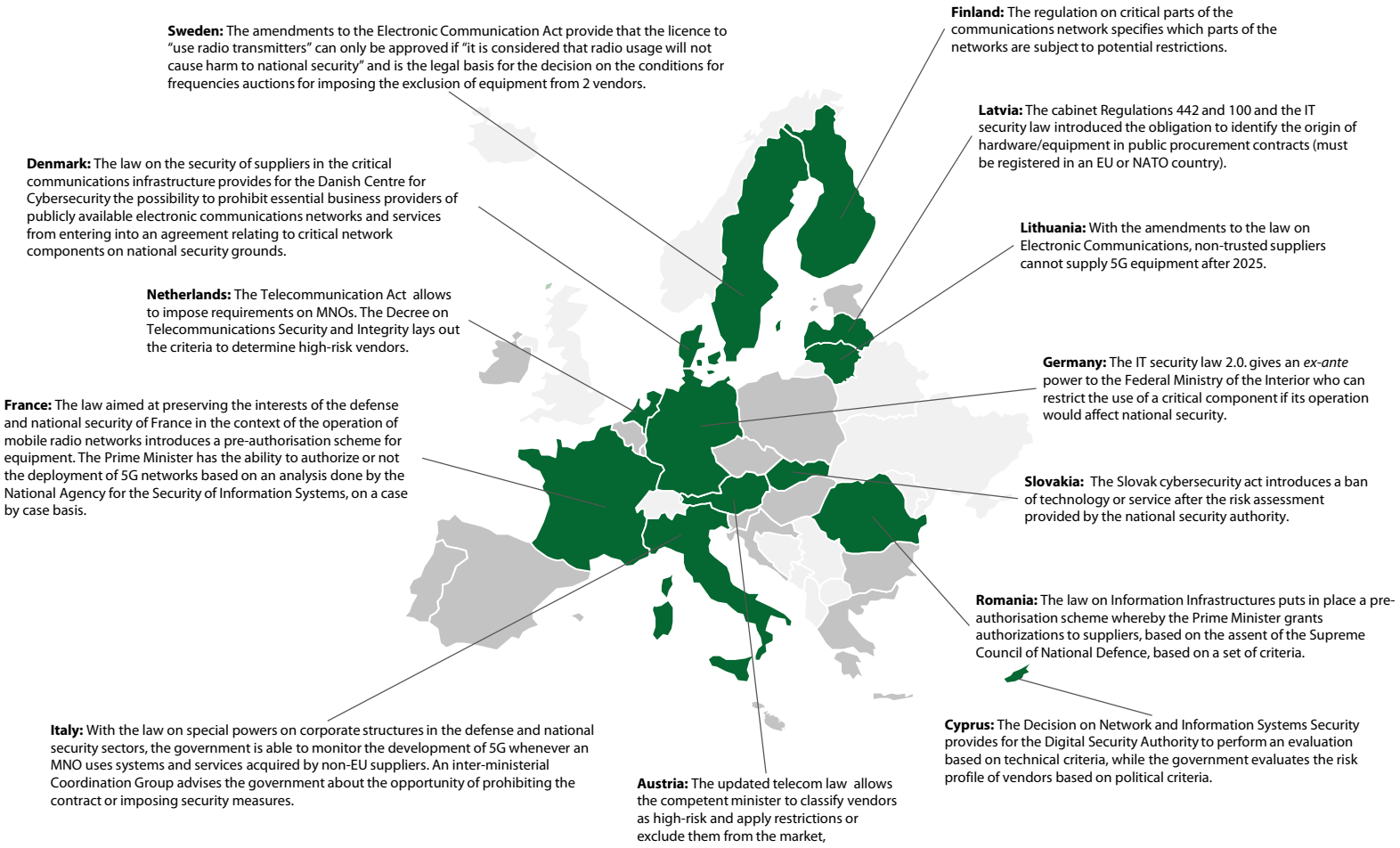
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(5) https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf

(6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/hungary

75 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. By the end of 2021, 13 Member States have adopted or amended national laws on 5G security. These regulatory measures take account of the criteria set out in the toolbox, but follow different approaches (see ***Figure 6***). Other Member States are in the process of tabling such legislation. In the years to come this may lead to more convergent approaches towards high-risk 5G vendors, at least among those Member States that have enacted such legislation.

Figure 6 – Member States that have adopted laws enabling to exclude equipment from high-risk vendors from their networks, October 2021



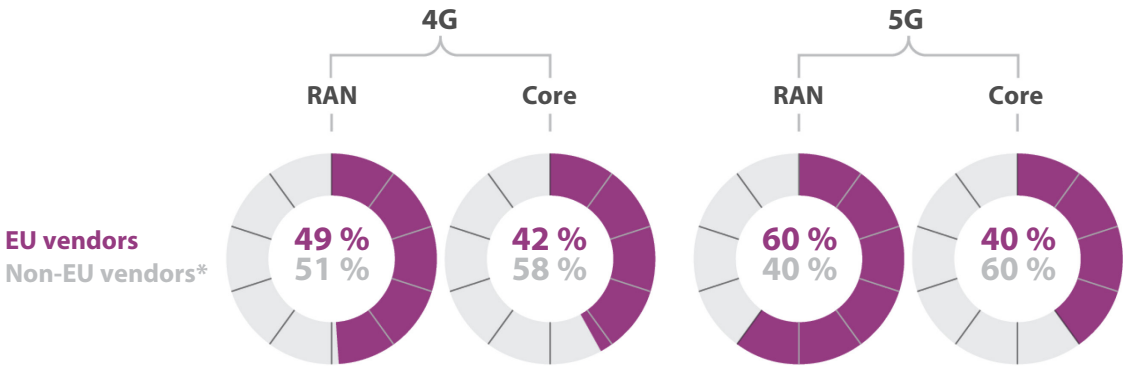
Source: ECA, based on European Commission data.

76 So far, the Commission has not assessed what the impact of such divergent approaches would be, where one Member State builds its 5G networks using equipment from a vendor considered to be high-risk in another Member State. This could impact either cross-border security or competition between MNOs operating in the EU single market.

The Commission has recently started addressing the issue of foreign subsidies distorting the internal market

77 As of December 2020, more than half of all 4G and 5G equipment in the EU was being sourced from non-EU vendors (see ***Figure 7***).

Figure 7 – Share of MNOs using EU/non-EU* vendors' equipment



* *non-EU includes North America, Asian and Australian vendors.*

Source: ECA, based on BEREC. Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience). BoR (20) 227.

78 In particular, as of the end of 2019, 286 million customers in the EU 27 (64 % of the total population) were using telecommunication networks based on Chinese vendors' 4G equipment[59]. In October 2020, a group of MEPs raised concerns to Member State telecom and trade ministers and the Commission that one of the reasons for the large market share of Chinese vendors was that they benefitted from an unfair economic advantage, i.e. they received public subsidies that are not available for EU vendors under the EU's state aid rules[60]. In a recent review, we highlighted

[59] StrandConsult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks.

[60] Letter from MEPs to EU telecom and trade ministers and to European Commissioners Thierry Breton, Margrethe Vestager and Valdis Dombrovskis, 14.10.2020.

similar risks in this regard[61]. Such subsidies may distort the internal market, thereby creating an unlevel playing field amongst 5G vendors, with possible security implications. In May 2021, to tackle this problem, the Commission proposed a new Regulation[62], which lays down procedures for investigating such subsidies and redressing the associated market distortions.

The Commission does not have sufficient information regarding possible substitution costs for Chinese vendors' equipment

79 According to a June 2020 report[63], restricting a key vendor of 5G infrastructure in the EU would increase total investment costs by almost €2.4 billion per year over the next decade (i.e. €24 billion). According to a different study[64], European operators are already facing the upgrade of 4G networks built between 2012 and 2016, because it is standard business practice to overhaul and modernise network equipment which is more than three to four years old. This study estimates that the total cost to 'rip and replace' upgradable equipment bought from Chinese vendors since 2016 will be about €3 billion.

80 The high share of equipment from Chinese vendors, combined with their possible categorisation as high-risk in certain Member States, may lead to substitution costs in the order of billions of euros if MNOs needed to remove and replace Chinese vendors' equipment from European networks without a transitional period (see paragraphs ***77*** to ***79***). In principle, state aid cannot be granted to compensate operators for fulfilling legal obligations, unless Member States can demonstrate to the Commission that the necessary requirements are fulfilled (such as an incentive effect). Our analysis has identified one case where national laws might allow substitution costs to be supported by national public funding (see the Finnish Act on Electronic Communications Services[65]). Member States are required to notify the Commission of any case of state aid to compensate MNOs for such costs. According to the Commission, so far no Member State or stakeholder has contacted them to discuss state aid for equipment substitution costs. According to industry stakeholders interviewed during the audit,

---

[61] ECA review 03/2020: The EU´s response to China´s state-driven investment strategy.

[62] Proposal for a Regulation on foreign subsidies distorting the internal market, COM(2021) 223 final of 5.5.2021.

[63] Oxford Economics, Restricting competition in 5G network equipment throughout Europe, June 2020. (Sponsored by Huawei).

[64] StrandConsult, The real cost to 'rip and replace' Chinese equipment from telecom networks.

[65] Act on Electronic Communications Services 1207/2020 of 30.12.2020, article 301.

uncertainty about the treatment of such costs by Member States, and possible differences between Member States, undermine business certainty and risk impacting the timely deployment of 5G.

Conclusions and recommendations

81 Overall, our audit showed that, despite the Commission's support, there are considerable delays in the Member States' deployment of 5G networks and further efforts are necessary to address security issues in 5G deployment.

82 In its 2016 5G Action Plan, the Commission called for a 5G coverage of all urban areas and along main transport paths by 2025 and, in March 2021, for a full coverage by 2030. As of the end of 2020, 23 Member States had launched commercial 5G services and had achieved the intermediary objective of having at least one major city with access to such services. However, we found that not all Member States refer to the Commission objectives in their national 5G strategies or broadband plans. Moreover, in several countries the European Electronic Communications Code has not yet been transposed into national law and the assignment of 5G spectrum was delayed. These delays in assigning the spectrum can be attributed to different reasons: a weak demand by mobile network operators (MNOs), cross-border coordination issues with non-EU countries along the eastern borders, the impact of COVID-19 on auction schedules and uncertainty on how to deal with security issues. According to the Commission, only 11 Member States are likely to achieve the 2025 objective (see paragraph ***22*** to ***43***).

83 The Commission has supported Member States in their implementation of the 2016 5G Action Plan through initiatives, guidance and the funding of 5G-related research. However, the Commission did not define the expected quality of service of 5G networks, such as the performance it should offer in terms of minimum speed and maximum latency. This has led to the term "5G quality" being understood differently by Member States. We noted divergent approaches by Member States in the deployment of 5G services, such as the fact that only two Member States have defined minimum speed and maximum latency. Ultimately these divergent approaches carry the risk of inequalities in the access and quality of 5G services in the EU, thereby increasing rather than reducing the "digital divide" between Member States and regions (see paragraphs ***22*** to ***31***).

Recommendation 1 – Promote the even and timely deployment of 5G networks within the EU

The Commission should:

(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;

(b) encourage Member States to include the 2025 and 2030 objectives for 5G deployment, and the measures that will be needed to achieve them, in the next updates of their 5G/digital strategies or broadband plans; and

(c) support Member States in addressing spectrum coordination issues with neighbouring non-EU countries, for example by advocating that the topic is on the agenda of each relevant meeting.

Timeframe: December 2022

84 The security aspects of 5G networks only recently became a major concern at EU level. The associated need for action at EU level was highlighted by the European Council in 2019, where it called for a concerted approach and cooperation among Member States on this cross-border topic. The Commission, together with Member States, reacted swiftly to emerging 5G security concerns. In 2020, the NIS Cooperation Group adopted an EU toolbox on 5G cybersecurity which specifies a number of strategic, technical and support measures to deal with 5G security networks threats and identifies the actors responsible for each of these measures. Several of the measures address the issue of high-risk vendors of 5G equipment. This toolbox was subsequently endorsed by the Commission and the European Council (see paragraphs ***45*** to ***47***). As the toolbox is a soft law instrument, these measures have no binding effect on Member States. More recently, the EU toolbox on 5G cybersecurity, has been mentioned, in the new European Strategy to boost smart, clean and secure links in digital systems across the world, as a tool to guide investments in digital infrastructure (see paragraph ***50***).

85 The criteria in the toolbox offer an operational framework that is useful for assessing the risk profile of suppliers in a coordinated manner across all Member States. At the same time, carrying out this assessment remains a national responsibility (see paragraph ***54***).

86 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. By October 2021, taking account of this framework, 13 Member States have enacted or amended legislation on 5G security. Other Member States are in the process of tabling legislation that takes account of the toolbox criteria (see paragraph ***54*** and ***75***).

87 The toolbox was adopted at an early stage of the 5G deployment, but a number of MNOs had already selected their suppliers for 5G equipment (see paragraph ***52***). Not addressing security concerns from the design of a policy risks having a negative impact on its implementation, such as that the expected benefits (for example growth of GDP) could be eroded by the cost of dealing with threats (for example cost of cybercrime) (see paragraphs ***02*** and ***04***).

88 The toolbox takes into account national competences and relevant country-specific factors. Our audit showed that, so far, Member States have applied divergent approaches regarding the use of equipment from high-risk vendors or the scope of the restrictions (for example core or critical parts of the 5G network only, or radio access network or part of it) (see paragraphs ***74*** and ***75***).

89 In the years to come, legislation on 5G security enacted by Member States based on the toolbox may lead to more convergent approaches towards high-risk 5G vendors. However, as none of the measures set out in this toolbox are legally binding, the Commission has no power to enforce them. Therefore, there remains a risk that the toolbox in itself cannot guarantee that Member States address security aspects in a concerted manner (see paragraph ***49*** *to* ***75***).

90 Many 5G vendors are located outside the EU and thus operating within the framework of third-country legislations, which can differ considerably from the EU standards, for example in terms of effective data protection accorded to citizens, and more generally on how judicial independence is ensured by legislative or democratic checks and balances. The fact that 5G networks are pre-dominantly software-run may also be a particular security concern if control centres of such software are placed in non-EU countries, potentially subjecting EU citizens to third country legislation. The Commission has started addressing these concerns, considering that any business providing services to EU citizens should respect the EU rules and values. It has also started dialogues with several countries to secure strong privacy protection for personal data (see paragraphs ***56*** to ***62***).

91 Despite the cross-border nature of 5G security concerns, there is a lack of public information available on how Member States approach security matters and their reliance on high-risk vendors. The Commission tracks and reports on the implementation of the toolbox. How ever, the reports do not present detailed and comparable information on how Member States approach 5G security concerns. Furthermore, as of September 2021, no future reporting is planned. This lack of information hampers knowledge sharing between Member States and the possibility to apply concerted measures. It also limits the possibility for the Commission to propose improvements to the security of 5G networks (see paragraphs ***68*** to ***73***).

Recommendation 2 – Foster a concerted approach to 5G security among Member States

The Commission should:

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

Timeframe: December 2022

(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.

Timeframe: December 2022

(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.

Timeframe: December 2022

92 The Commission has started addressing the associated allegations of unfair economic advantage due to foreign subsidies. Such subsidies may distort the internal market, thereby creating an unlevel playing field amongst 5G vendors, with possible security implications (see paragraph ***78***).

93 The Commission does not have sufficient information on Member States' treatment of potential substitution costs that could arise if MNOs need to remove high-risk vendors' equipment from EU networks without a transitional period. Differences in treatment may undermine business certainty and risk impacting the timely deployment of 5G (see paragraphs ***79*** and ***80***). At the same time, Member States' approaches towards 5G security, and in particular the absence of a concerted approach across the EU, may impact the effective functioning of the single market. So far, the Commission has not assessed this issue (see paragraphs ***74*** to ***76***).

Recommendation 3 – Monitor Member States' 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.

Timeframe: December 2022

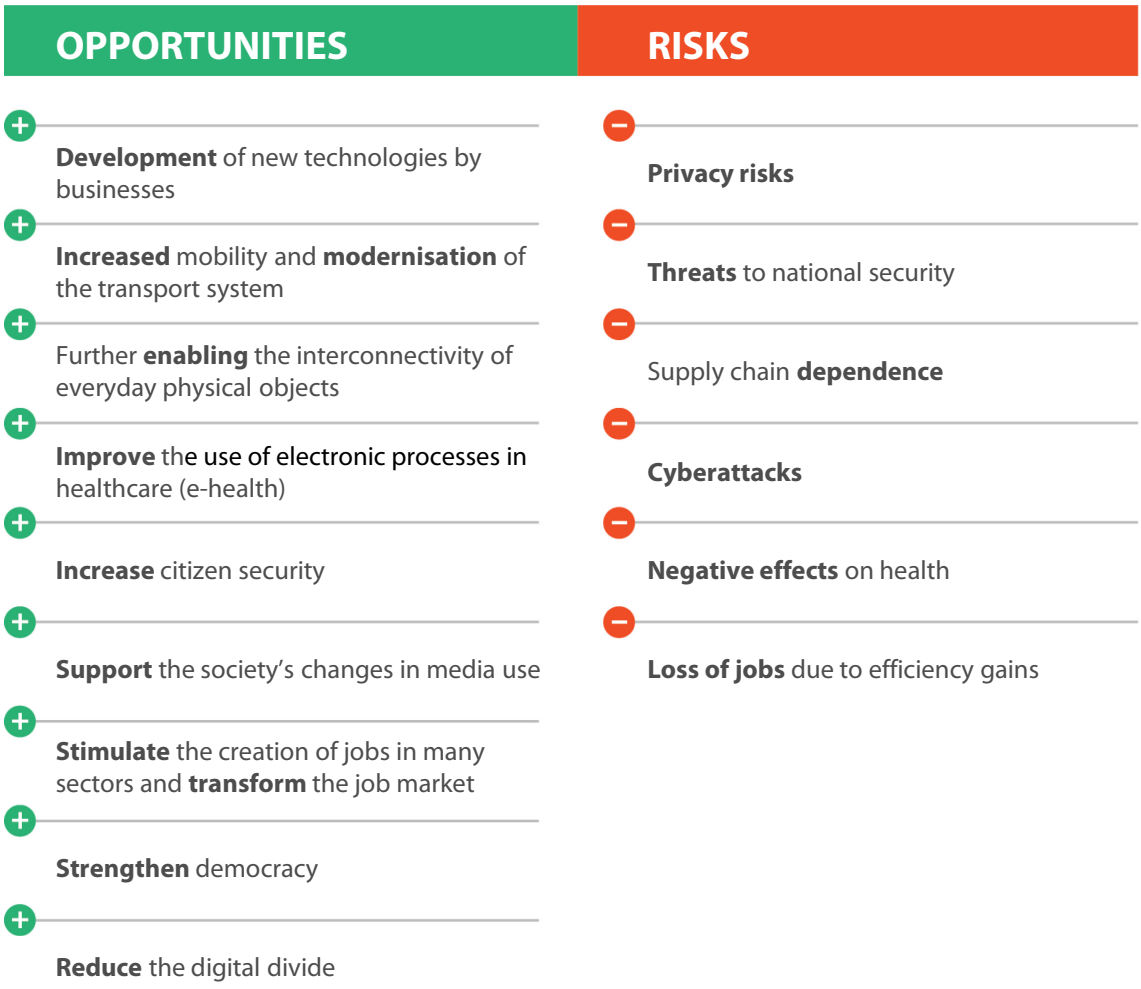
This Report was adopted by Chamber II, headed by Ms Iliana Ivanova, Member of the Court of Auditors, in Luxembourg on 15 December 2021.

For the Court of Auditors

Klaus-Heiner Lehne
President

Annexes

Annex I – Main 5G opportunities and risks



Source: ECA, based on European Parliamentary Research Service – European Science-Media hub.

Annex II – Examples showing the impact of telecom network disruption and cybersecurity incidents

France emergency call numbers failure[66, 67]

01 On 3rd June 2021, a network outage at Orange, France's biggest telecom company, prevented emergency calls for a period of several hours. While a cyberattack has been ruled out as the cause, the incident demonstrates the potential impact of disruption to a critical network infrastructure.

Irish public healthcare ransomware attacks[68, 69, 70]

02 In May 2021, Ireland's health service (the Health Service Executive) shut down all its IT systems because of a ransomware attack. The attack affected all aspects of patient care as it created difficulties in accessing patient records, increasing the risk of delays and errors. While Irish officials are not aware that any patient data was compromised, the sharing of health records could have led to all types of contingent crimes such as fraud and blackmail. According to the Health Service Executive Director-General, the estimated recovery costs are likely to total €500 million ($600 million).

---

66 https://www.euronews.com/2021/06/03/french-telecom-operator-orange-apologises-after-emergency-numbers-crash-nationwide

67 https://www.reuters.com/business/media-telecom/orange-blames-network-outage-software-failure-audit-2021-06-11/

68 https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875

69 https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

70 https://www.cert.europa.eu/cert/moreclusteredition/en/blog_DataBreachTodayinRSSSyndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds[71, 72, 73]

03 Solarwinds is an American company that develops software to help businesses and state and federal agencies to help manage their networks, systems, and information technology infrastructure. In early 2020, Solarwinds was the object of a software attack. The hackers managed to spread the attacks to Solarwinds' clients through software upgrades containing malicious codes. These opened backdoors in the clients' platforms, affording easy entry for attacks and the installation of further malware and spyware.

[71] https://www.solarwinds.com/

[72] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[73] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

Annex III – Legal and policy framework

European Commission

European Council Council of the EU

Legislation

NIS Cooperation Group

2016 – NIS Directive, July 2016 – Providing legal measures to boost the overall level of cybersecurity in the EU.

2016 – 5G Action Plan, September 2016 – Aiming at launching 5G services in all Member States by end 2020 at the latest, followed by a rapid build-up to ensure uninterrupted 5G coverage in urban areas and along main transport paths by 2025.

2018 – Electronic Communications Code, December 2018 – Aiming at implementing an internal market in electronic communications networks and services.

2019 – European Council conclusions, March 2019 – Looking forward to the Commission's recommendation on a concerted approach to the security of 5G networks.

2019 – Recommendation on 5G cybersecurity, March 2019 – Recommending Member States to assess the cybersecurity risks affecting 5G networks at national level and take necessary security measures.

2019 – Council conclusions on the significance of 5G to the European Economy, December 2019 – Emphasising that a swift and secure roll-out of the 5G networks is key for enhancing the competitiveness of the EU and requires a coordinated approach in the EU.

2020 – 5G cybersecurity toolbox, January 2020 – Identifying a possible common set of measures, which are able to mitigate the main cybersecurity risks of 5G networks.

2020 – Secure 5G deployment in the EU – Implementing the EU 5G cybersecurity toolbox, January 2020 – The European Commission endorsing the toolbox and setting out its next steps (e.g. a report on implementation by June 2020).

2020 – Council conclusions on Shaping Europe's Digital Future, June 2020 – Supporting the need to ensure and implement a coordinated approach to mitigate the main risks for a secure 5G deployment in the EU.

2020 – European Council conclusions, October 2020 – Endorsing the 5G cybersecurity toolbox, in particular the need to apply the relevant restrictions on high-risk suppliers.

2020 – Recommendation for (…) access to 5G radio spectrum, September 2020- Setting out guidance for developing best practices for fostering connectivity and provide timely and investment-friendly access to 5G radio spectrum.

2020 – The EU's Cybersecurity Strategy for the Digital Decade, December 2020 – A 'soft law' document, setting out the Commission priorities and planned actions for cybersecurity as a whole, including 5G networks.

2020 – Proposal for a NIS 2 Directive, December 2020 – Aiming to modernize and enlarging the scope of the current directive, also covering 5G cybersecurity more explicitly.

2020 – Proposal for a Directive on the resilience of critical entities, December 2020 – Aiming to reduce vulnerabilities of critical infrastructures that are essential for the functioning of the EU's society and economy.

2020 – 2030 Digital Compass: the European way for the Digital Decade, March 2021 – Mapping out a path towards a common vision and actions for Europe to succeed in the Digital Decade.

2021 – Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade, March 2021 – Supporting the next steps to be taken on the cybersecurity of 5G networks, as set out by the Commission's cybersecurity strategy.

Annex IV – Examples of EFSI co-funded projects

EFSI 5G related projects

The two EFSI projects that we reviewed concerned the research, development and innovation investments for the development of 5G network product portfolios. They covered the development of hardware and software for the Radio Access Network as well as for the Core network. Both projects contributed to denser cell deployment, supported standardisation and facilitated key technology experiments.

The projects started in 2018 and ended in December 2020. They had combined total investment costs of €3.9 billion, including €1 billion in financing from EFSI.

Annex V – Examples of Horizon 2020 and ERDF projects

Horizon 2020 5G related project

This project uses equipment from all the three main 5G vendors (Ericsson, Huawei and Nokia) to test 5G technologies in the cross-border corridor connecting the cities of Metz (France), Merzig (Germany) and Luxembourg. It started in November 2018 and was planned to run for 31 months. The EU granted €12.9 million towards the overall total budgeted of €17.1 million.

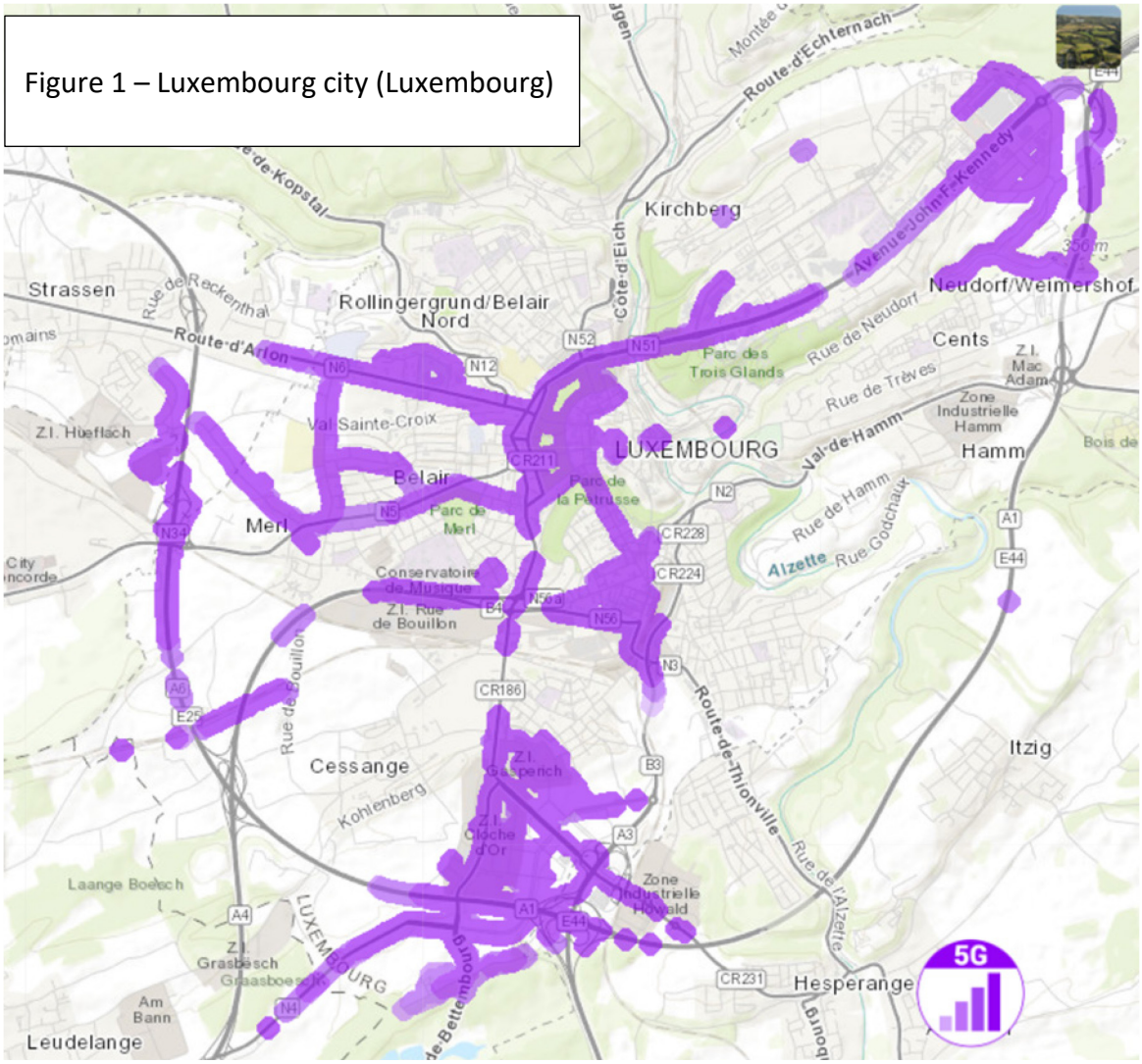
ERDF 5G related project

This project in Spain aims to provide insights on 5G network deployments. It includes experimenting with network management techniques enabled by 5G technology, such as network virtualisation, edge computing, dynamic network service allocation and network slicing, and developing 5G use cases. The project started in 2019 and was planned to last for 30 months. The EU contribution is €2.2 million out of the total expected cost of €7.1 million.

Annex VI – 5G coverage in selected cities

The figures below are based on data on mobile broadband connectivity collected from tests carried out by users of the Nperf app. The areas where 5G has been detected are not necessarily commercially open. As the network performance depends on the individual MNOs, the following maps, extracted on 4 October 2021, only show coverage, and not performance such as speed and latency.

Figure 1 – Luxembourg city (Luxembourg)



© nPerf.

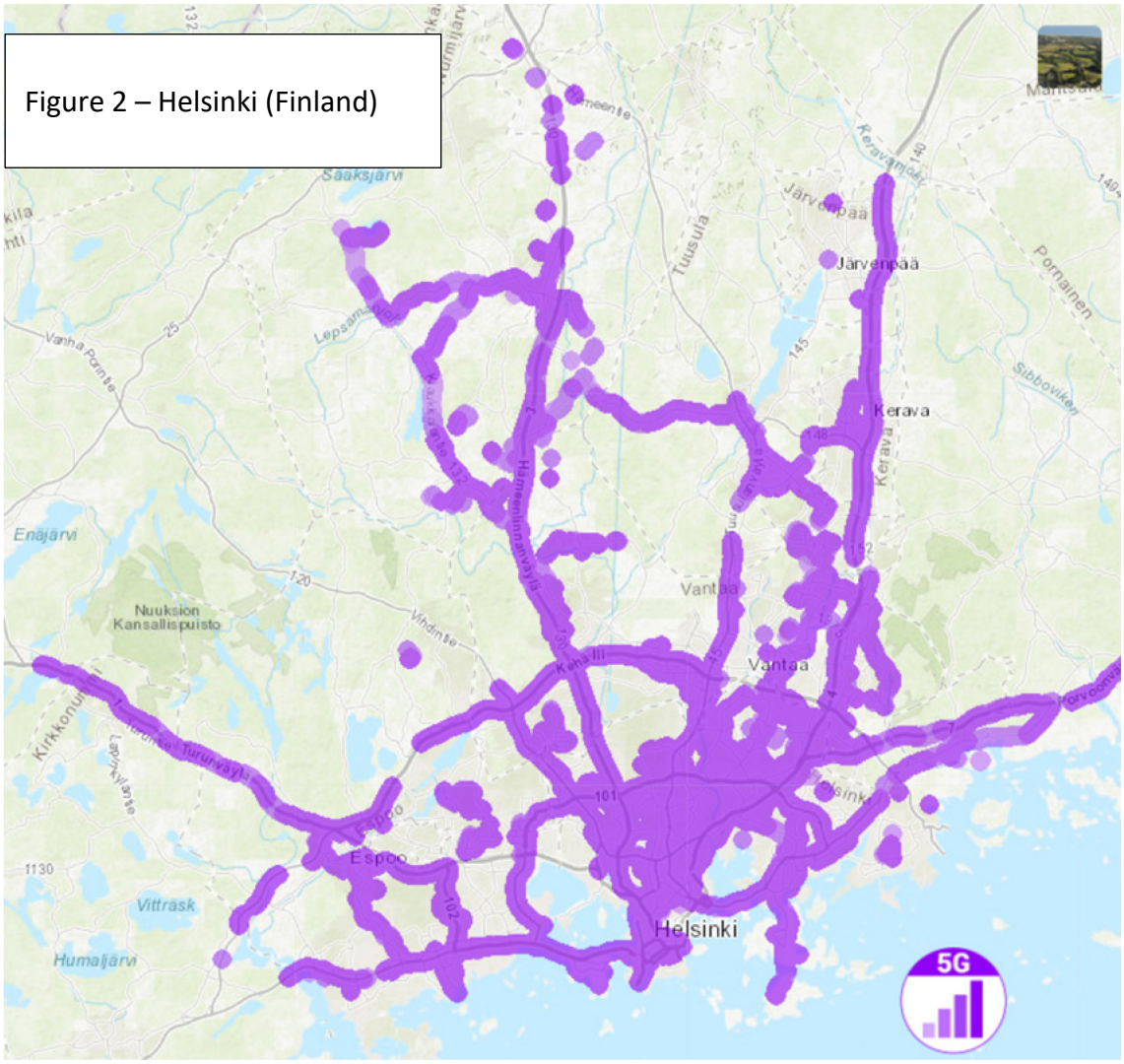


Figure 2 – Helsinki (Finland)

© nPerf.

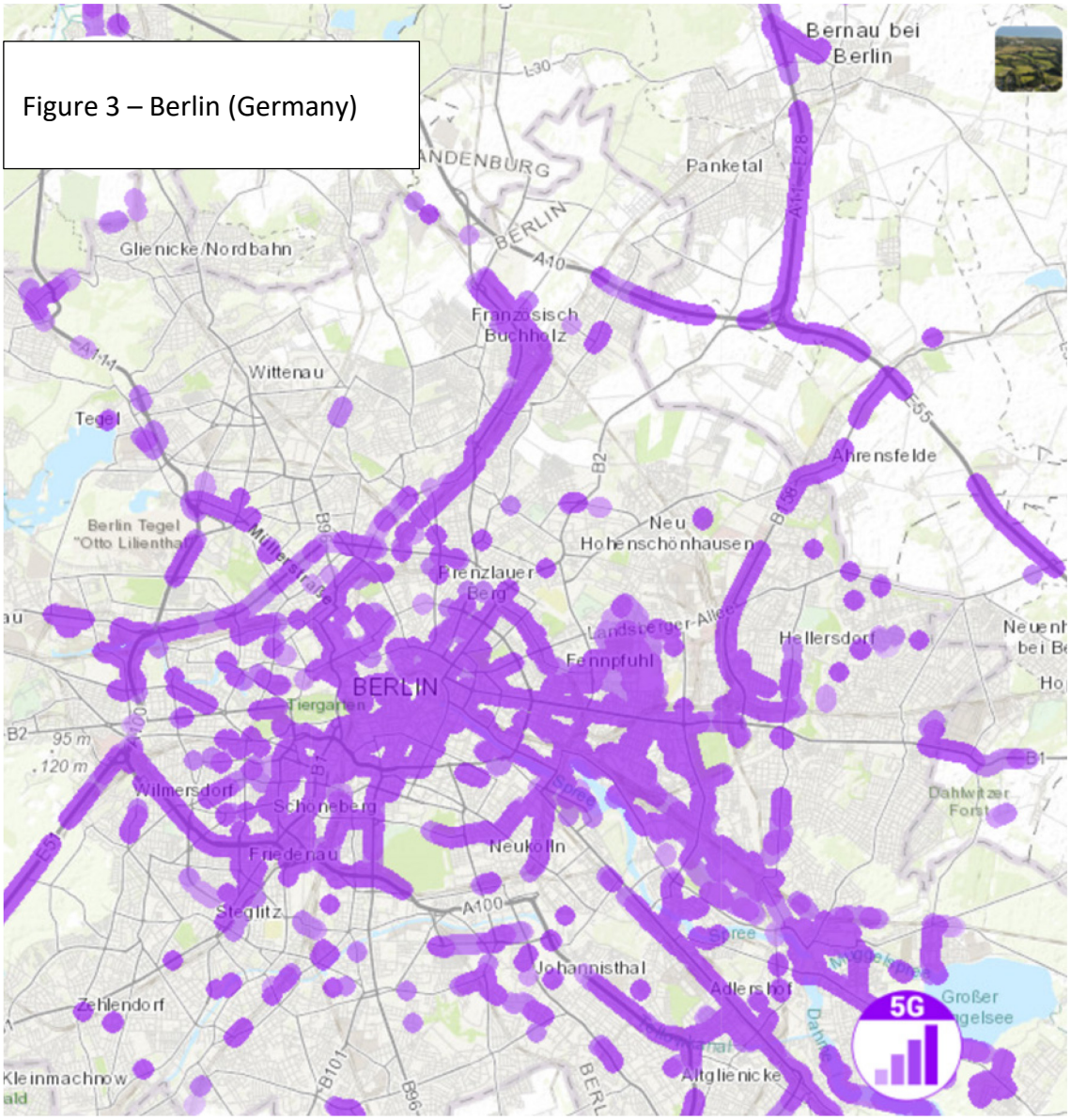


Figure 3 – Berlin (Germany)

© nPerf.

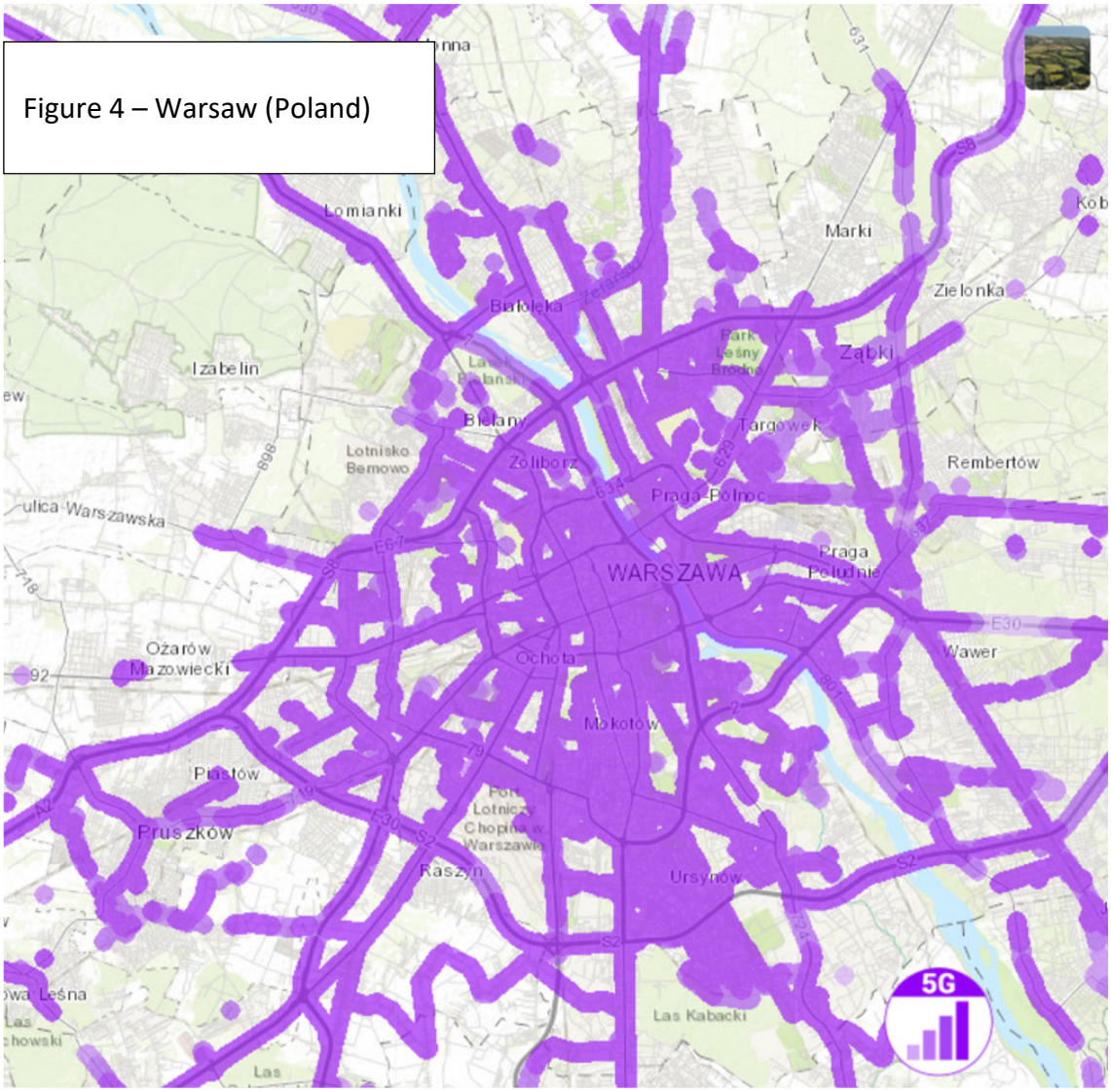


Figure 4 – Warsaw (Poland)

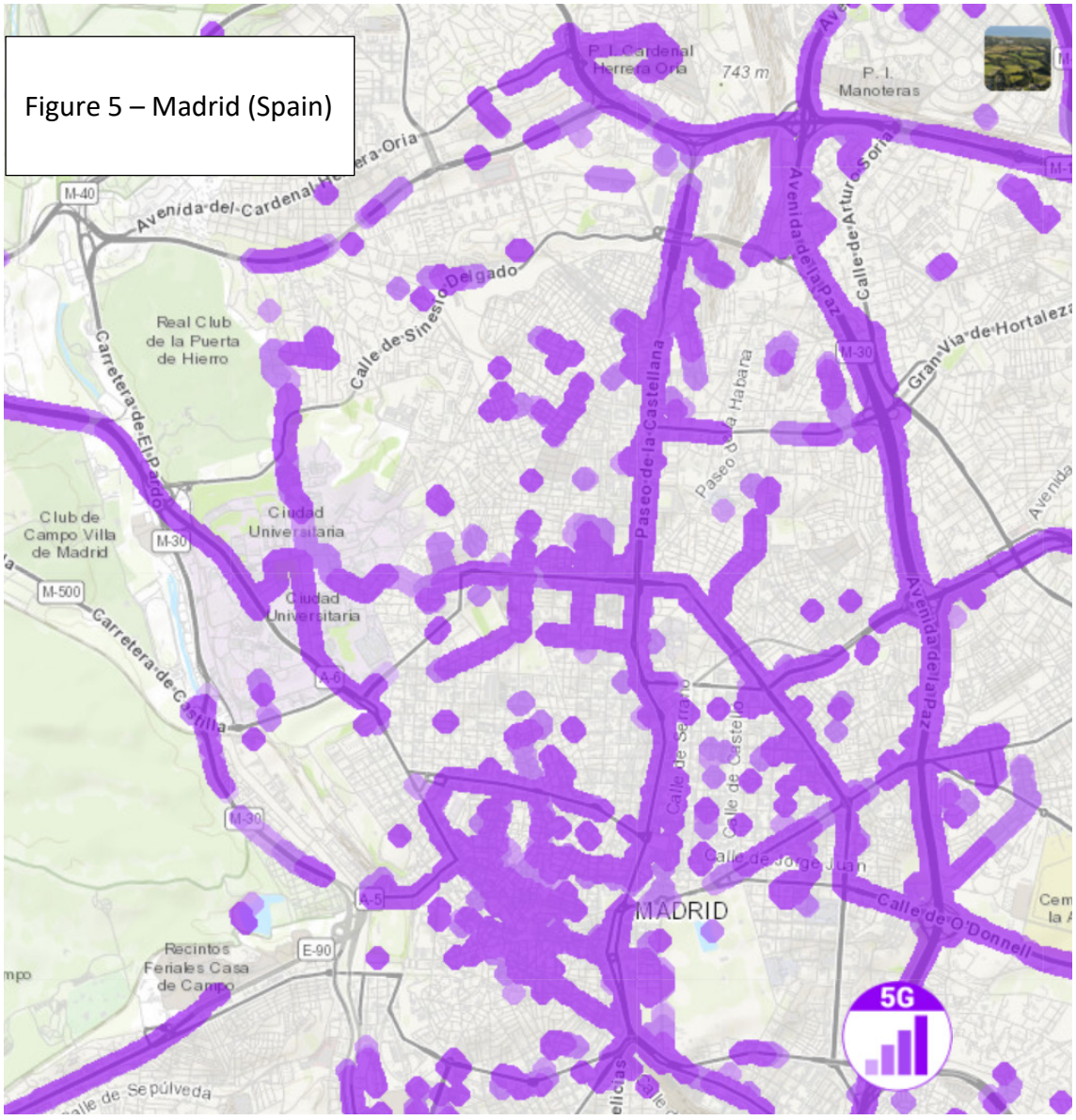


Figure 5 – Madrid (Spain)

Annex VII – EU toolbox on 5G cybersecurity

The EU toolbox on 5G cybersecurity, adopted by the NIS Cooperation Group and endorsed by the Commission, contains three types of non-binding measures (strategic, technical and support measures) to be implemented by various actors, as summarised below.

Measures	Relevant actors				
	Member States authorities	MNOs	European Commission	ENISA	Stakeholders (incl. suppliers)
Strategic measures					
SM01 – Strengthening the role of national authorities	✓	✓			
SM02 – Performing audits on operators and requiring information	✓	✓			
SM03 – Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk – including necessary exclusions to effectively mitigate risks- for key assets	✓	✓			
SM04 – Controlling the use of Managed Service Providers and equipment suppliers' third line support	✓	✓			
SM05 – Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies	✓	✓			
SM06 – Strengthening the resilience at national level	✓	✓			
SM07 – Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU	✓		✓		
SM08 – Maintaining and building diversity and EU capacities in future network technologies	✓		✓		✓
Technical measures					
TM01 – Ensuring the application of baseline security requirements (secure network design and architecture)	✓	✓			
TM02 -Ensuring and evaluating the implementation of security measures in existing 5G standards	✓	✓			✓
TM03 – Ensuring strict access controls	✓	✓			
TM04 – Increasing the security of virtualised network functions	✓	✓			
TM05 – Ensuring secure 5G network management, operation and monitoring	✓	✓			
TM06 – Reinforcing physical security	✓	✓			

Measures	Relevant actors				
	Member States authorities	MNOs	European Commission	ENISA	Stakeholders (incl. suppliers)
TM07 – Reinforcing software integrity, update and patch management	✓	✓			
TM08 – Raising the security standards in suppliers' processes through robust procurement conditions	✓	✓			✓
TM09 – Using EU certification for 5G network components, customer equipment and/or suppliers' processes	✓	✓	✓	✓	✓
TM10 – Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)	✓		✓	✓	✓
TM11 – Reinforcing resilience and continuity plans	✓	✓			✓
Supporting actions					
SA01 – Reviewing or developing guidelines and best practices on network security	✓	✓		✓	
SA02 – Reinforcing testing and auditing capabilities at national and EU level	✓		✓	✓	
SA03 – Supporting and shaping 5G standardisation	✓	✓	✓	✓	✓
SA04 – Developing guidance on implementation of security measures in existing 5G standards	✓			✓	
SA05 – Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme	✓			✓	✓
SA06 Exchange of best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers	✓				
SA07 – Improving coordination in incident response and crisis management	✓			✓	
SA08 – Conducting audits of interdependencies between 5G networks and other critical services	✓				
SA09 – Enhancing cooperation, coordination and information sharing mechanisms	✓			✓	
SA10 – Ensuring 5G projects supported with public funding take into account cybersecurity risks	✓		✓		

Source: EU toolbox on 5G cybersecurity.

Acronyms and abbreviations

BEREC: Body of European regulators for electronic communications

EECC: European Electronic Communications Code

EFSI: European Fund for Strategic Investments

EIB: European Investment Bank

ENISA: European Network and Information Security Agency

ERDF: European Regional Development Fund

GDP: Gross domestic product

MNO: Mobile network operator

NBP: National broadband plan

NIS: Network and Information System

RAN: Radio access network

RRF: Recovery and Resilience Facility

RSPG: Radio Spectrum Policy Group

Glossary

Body of European Regulators for Electronic Communications: Body, composed of representatives of Member States' national regulatory authorities, which assists those authorities and the Commission in implementing the EU's regulatory framework with a view to creating a single market for electronic communications.

Broadband: High-speed, simultaneous transmission of multiple information formats (such as data, voice and video).

European Fund for Strategic Investments: Investment support mechanism launched by the European Investment Bank (EIB) and the Commission, as part of the Investment Plan for Europe, to mobilise private investment in projects of strategic importance for the EU.

European Union Agency for Cybersecurity: EU agency set up to develop and maintain a high level of network and information security in all sectors of private and public life.

Exabyte: A measure of digital information storage capacity, equivalent to 1 billion gigabytes.

Global System for Mobile Communications Association (GSMA): Industry organisation that represents the interests of mobile operators worldwide, as well as manufacturing and service companies and organisations with an interest in mobile infrastructure.

Internet of things: Physical objects embedded with sensors, software and other technologies which enable them to connect wirelessly and exchange data with other devices and systems.

Latency: In computer networks, the time required for a set of data to travel between two points.

Mobile network operator: Telecommunications company that provides wireless voice and data communication for subscribed mobile phone users.

National broadband plans: Member States documents containing strategic objectives for achieving the EU's broadband targets.

Network and Information Systems Cooperation Group: Body established by the NIS Directive to ensure cooperation and information exchange among Member States and composed of representatives of the EU Member States, the European Commission and the EU Agency for Cybersecurity.

Radio access network: A major part of modern telecommunications technology, linking individual devices to other parts of a network through radio connections.

Radio Spectrum Policy Group: High-level advisory group, composed of Member State representatives, that assists and advises the EU institutions on development of the single market in wireless products and services.

Radio spectrum: The part of the electromagnetic spectrum corresponding to radio frequencies.

Ransomware: Malware that denies victims access to a computer system or makes files unreadable, forcing the victim to pay a ransom to restore access.

Replies of the Commission

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60614

Timeline

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60614

Audit team

The ECA's special reports set out the results of its audits of EU policies and programmes, or of management-related topics from specific budgetary areas. The ECA selects and designs these audit tasks to be of maximum impact by considering the risks to performance or compliance, the level of income or spending involved, forthcoming developments and political and public interest.

This performance audit was carried out by Audit Chamber II Investment for cohesion, growth and inclusion spending areas, headed by ECA Member Iliana Ivanova. The audit was led by ECA Member Annemie Turtelboom, supported by Florence Fornaroli, Head of Private Office and Celil Ishik, Private Office Attaché; Niels-Erik Brokopp, Principal Manager; Paolo Pesce, Head of Task; Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov, and Nils Westphal, Auditors.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7413-5	ISSN 1977-5679	doi:10.2865/011861	QJ-AB-21-029-EN-N
HTML	ISBN 978-92-847-7383-1	ISSN 1977-5679	doi:10.2865/681201	QJ-AB-21-029-EN-Q

5G is expected to add up to €1 trillion to the European GDP between 2021 and 2025, with the potential to create or transform up to 20 million jobs across all sectors of the economy. We observed that delays are putting at risk the achievement of the EU's objectives for 5G deployment and that further efforts are necessary to address security issues. In the report, we make a number of recommendations to the Commission aimed at pushing forward the timely and concerted implementation of secure 5G networks in the EU.

ECA special report pursuant to Article 287(4), second subparagraph, TFEU.

CURIA RATIONUM

EUROPEAN
COURT
OF AUDITORS

Publications Office
of the European Union

EUROPEAN COURT OF AUDITORS
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Enquiries: eca.europa.eu/en/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors