

# **DIGITALISATION UNDER SURVEILLANCE** THE DEVELOPMENT OF THE 5G NETWORK IN RUSSIA

Iwona Wiśniewska



WARSAW OCTOBER 2020

## **DIGITALISATION UNDER SURVEILLANCE** THE DEVELOPMENT OF THE 5G NETWORK IN RUSSIA

Iwona Wiśniewska



© Copyright by Centre for Eastern Studies

CONTENT EDITORS Adam Eberhardt, Marek Menkiszak

EDITOR Małgorzata Zarębska

CO-OPERATION Szymon Sztyk, Katarzyna Kazimierska

TRANSLATION OSW

CO-OPERATION Nicholas Furnival

CHARTS Urszula Gumińska-Kurek

MAP Wojciech Mańkowski

GRAPHIC DESIGN PARA-BUCH

DTP IMAGINI

PHOTOGRAPH ON COVER Gorodenkoff / Shutterstock.com



Centre for Eastern Studies ul. Koszykowa 6a, 00-564 Warsaw, Poland tel.: (+48) 22 525 80 00, info@osw.waw.pl

ISBN 978-83-65827-57-9

#### Contents

### MAIN POINTS | 5

### I. THE DIGITAL SECTOR OF THE RUSSIAN ECONOMY | 7

- 1. Current state of the development of the digital economy in Russia | 7
- 2. State involvement in the sector | 8
- 3. Subordination of digitalisation to the security agenda | 12
- 4. The regulatory framework of the digital transformation  $|\ \mathbf{16}$
- 5. Selected actors involved in the "Digital Economy" national programme | **18**
- 6. Financing the "Digital Economy" programme | 22

## II. RUSSIA'S 5G NETWORK DEVELOPMENT PLANS | 25

- 1. The current state of the mobile market in Russia | 25
- 2. The development of the 4G network in Russia | 27
- 3. Russia's 5G network development plans | 31
- 4. 5G network testing | 34
- 5. Works on the 'concept for the creation and development of the 5G/IMT-2020 network in Russia' | **36** 
  - 5.1. The vision of the 5G network as proposed by the Ministry for Digital Development | **36**
  - 5.2. Criticisms of the draft concept for the development of the 5G network | **38**
- 6. The dispute over radio frequencies for the 5G network | 41
  - 6.1. The main new radio frequency bands necessary for the development of 5G networks | **41**
  - 6.2. Problems with access to the 700 MHz band in Russia | 43
  - 6.3. Limitations on access to the 3.4–3.8 GHz band in Russia | 46

### III. PROSPECTS OF RUSSIA'S DIGITAL TRANSFORMATION AND CONCLUSIONS | 49

APPENDICES | 54

#### MAIN POINTS

- The digital transformation has become one of the Russian government's economic priorities during Vladimir Putin's fourth presidential term. There are at least three reasons why the importance of the digital economy has been rising. Firstly, Russia has been promoting the digital transformation in reaction to the technological revolution taking place globally. The Kremlin has had to make Russia part of that process to prevent the gap between the Russian economy and that of the global economic leaders from widening. Secondly, the Russian government views the digital transformation as a new driver of economic growth that could replace Russia's current resource-based economic model which is close to exhausting its potential. Thirdly, as the digital transformation requires a large investment, for the most part financed from the federal budget, it offers new opportunities for the Russian political and business elite to gain access to public funds and enrich themselves.
- Russia's political model is based on the state having a strong role, central-٠ ised decision-making, corruption, and the dominance of the security forces. This has also determined the shape of the country's digital transformation. State-owned entities have a strong presence in the information and communication technology sector (ICT). The development of the digital sector has been dominated by security issues, which have turned out to be more important than technical or financial efficiency. The process has been significantly influenced by various actors striving to gain access to public funds and strengthen their positions in Russia's power structures. These include: Russia's major lobbyists (especially the Ministry of Defence and state-owned companies), and, to a lesser extent, the Ministry of Digital Development and private business. The fierce rivalry among the main actors vying to influence the course of the digital transformation has delayed the entire process, as a result of which the masterplan for the development of the digital economy in Russia is still in the formulation process.
- The development of ICT infrastructure, and especially the development of fifth-generation mobile networks (5G), has been a key area of Russia's digital transformation. Once launched, it will enable both mobile data speed and the number of devices that can be simultaneously connected to the network to be considerably increased, and in this way 5G is expected to revolutionise wireless communications and stimulate further the automation and digitalisation of economic processes. Those developments, in turn, are expected to boost Russia's economic growth. However, the development of

the 5G network is facing challenges which are a perfect illustration of the broader problems ahead of Russia's entire digital economy programme.

- The government has stated that it aims to initially develop 5G infrastructure in Russia's largest cities (with more than a million inhabitants) for selected economic sectors (these have not been identified at this stage). As with the entire digital transformation, the development of 5G infrastructure is expected to rely on Russian technologies, software and devices as much as possible. However, the current level of ICT technology development in Russia makes cooperation with foreign companies inevitable. In view of this, Russia has been trying to diversify its foreign business partners (Ericsson, Nokia, Huawei) and force them to locate at least some production facilities in Russia.
- A heated debate has been underway in Russia concerning two issues of crucial importance for the efficiency of the future 5G infrastructure: the operator market model and the choice of radio frequencies on which the network will operate. Most state-owned entities opt for a single, monopoly operator of the 5G infrastructure, while private companies are lobbying for a competitive model. Opinions on the choice of radio frequencies are also divided. Studies conducted in Russia confirm that the frequency ranges recognised as optimal by most countries in the world, i.e. 694-790 MHz, 3.4–3.8 GHz and 24.25–29.5 GHz, are the most promising for the development of the 5G network. However, they are currently in use, mostly by the security apparatus and digital television broadcasters, and are not accessible to mobile operators. For this reason, the government is currently suggesting that operators should develop the 5G network using the technologically less attractive 4.4–5 GHz band. As regards frequencies below 1 GHz, which are necessary for the development of the network especially outside major cities, decisions have been postponed for several reasons, including the fact that developing 5G networks here is not a priority for the Russian government in the initial phase.
- Successfully implementing at least parts of its digital transformation programme would be important for Russia's international position. The Kremlin likes to see Russia as an important player capable of influencing the global order. It would be interested in boasting about innovations and advanced technologies at least in selected economic sectors. Despite this determination, however, it is already clear that keeping the digital programme's deadlines, staying within the budget, and achieving the objectives set will pose a major challenge to the Russian authorities.

#### I. THE DIGITAL SECTOR OF THE RUSSIAN ECONOMY

# 1. Current state of the development of the digital economy in Russia

Russia's digital economy programme was officially launched in 2017 after the "Strategy for the development of the digital society in the Russian Federation for the years 2017–2030" was approved by a presidential decree. In reality, the digital transformation and the development of the IT sector started much earlier, although they grew in an unstructured manner. In particular, the development of the Russian internet (Runet) was very spontaneous in the 2000s and, combined with the expansion of ICT infrastructure (especially those built by private mobile operators) it created a strong foundation for the further digital transformation in Russia.

In early 2020, 118 million people in Russia, 81% of the population, had internet access. Social networks had 70 million active users, accounting for 48% of the population. An average internet user spent 7 hours and 17 minutes online a day (this includes listening to music and watching movies). The number of mobile internet users has been growing dynamically in Russia. In early 2020, 87% of internet users connected to the web using mobile devices, mostly smartphones (compared to 64% the year before).<sup>1</sup> In 2017, the number of those using mobile internet exceeded the number of those connecting from PCs for the first time.<sup>2</sup> The Russian Association for Electronic Communications (RAEC) offers different estimates, reporting that in December 2019 Runet had an audience of 96.7 million people, accounting for 97% of the population (the study covered only people above 12 years of age) and, of this number, more than 86 million connected via mobile devices.<sup>3</sup> The private operators have been competing for customers by offering low prices and, as a result, Russia is among the countries with the lowest prices of internet access.<sup>4</sup>

Estimates of the size of Russia's digital economy differ depending on the methodology adopted. The RAEC estimates that in 2019 the digital economy

<sup>&</sup>lt;sup>1</sup> S. Kemp, 'Digital 2020: The Russian Federation', DataReportal, 18 February 2020, www.datareportal.com.

<sup>&</sup>lt;sup>2</sup> Экономика Рунета 2018 / Цифровая экономика России 2018, Российская Ассоциация электронных коммуникаций (РАЭК), www.raec.ru.

<sup>&</sup>lt;sup>3</sup> <sup>(</sup>Рунет подвел итоги года: объем экономики Рунета составил 4,7 трлн рублей', РАЭК, 16 December 2019, www.raec.ru.

<sup>&</sup>lt;sup>4</sup> The monthly cost of a 100 Mbps internet access package was US\$ 7.68 in late 2019. M. Yarova, 'Countries with the cheapest and fastest Internet: price comparison', AIN.UA, 12 December 2019, www.ain.ua/en.

was worth RUB 6.4 billion, more than 6% of GDP, and had grown by 20% from  $2018.^{5}$  In a report by the Moscow Higher School of Economics drafted in cooperation with the government, the added value of the ICT sector in Russia in 2017 (the most recent data available) was estimated at less than 3% of GDP.<sup>6</sup>

Despite the progress of the digital transformation, Russia is not an innovation leader. It ranks among the 'moderate innovators' in the European Commission's assessment (Summary Innovation Index).<sup>7</sup> In the Bloomberg Innovation Index 2020, unveiled in January 2020, Russia ranks 26<sup>th</sup> among the 60 countries studied and scores a mere 68.6 points out of 100. Russia has climbed up one position from last year, but it is still 14 positions lower than it was in 2016. Over the last three years, the country has declined most in the areas of productivity, manufacturing added value, high-tech density (share of high-tech companies in overall market capitalisation). According to Bloomberg, the decline has been due to Western sanctions and dwindling oil prices.<sup>8</sup>

The Russian business also lags behind the world leaders with regard to the uptake of digital technologies. According to the Business Digitalisation Index published by the Higher School of Economics in Moscow (which measures the rate of businesses' adaptation to digital transformation in Russia, European countries, the Republic of Korea, and Japan), Russian companies can compete with global leaders only when it comes to broadband internet access. They lag behind in the uptake of the radio-frequency identification of persons and objects (RFID), enterprise resource planning (ERP) and e-commerce.<sup>9</sup>

#### 2. State involvement in the sector

The Russian ICT sector is considerably centralised with a strong state presence, which is the main source of investment in the sector (the federal budget is expected to provide around 70% of the funds needed to implement the digital programme). The state has been setting the speed of the digital transformation of society and business and pushing the transformation through the implementation of successive stages, including:

<sup>&</sup>lt;sup>5</sup> 'Экономика Рунета / Цифровая экономика России 2019', РАЭК, www.raec.ru.

Цифровая Экономика. Краткий статистический сборник, Высшая школа экономики, Москва 2019.

<sup>&</sup>lt;sup>7</sup> European Innovation Scoreboard 2019, European Commission, 17 December 2019, www.ec.europa.eu/ docsroom.

<sup>\* &#</sup>x27;Russia drops two places on Bloomberg innovation ranking', IntelliNews, 23 January 2019, www.intellinews.com.

<sup>9</sup> Д. Филатова, М. Кевеш, 'Индекс цифровизации бизнеса', Институт статистических исследований и экономики знаний (ИСИЭЗ), 27 February 2019, issek.hse.ru.

- the digitalisation of the tax service,
- the digitalisation of the cadastre,
- the electronic public procurement system,
- an electronic toll collection system for vehicles above 12 tons using federal roads (known as Platon),
- the National Track and Trace Digital System.

Those state programmes have been implemented mainly by state-owned businesses which have stepped up takeovers of private IT companies. The Stolypin Institute for the Economy of Growth estimates in its 2018 report (the most recent available) that in 2017, the state accounted for 35% of the combined capital of the ICT sector and for 49% of the content (e.g. text, images, data, audio and video files) and media sector. The state presence was the lowest (around 16%) in the IT services sector where small and medium-sized enterprises accounted for 46% of the market (based on service revenue). Still, the state played a key role in that sector because entities owned or co-owned by the state were the main contractors and largest consumers of IT services.<sup>10</sup> The presence of state-owned companies in the sector has expanded over the last two years with more takeovers of private companies and more public procurement.

The Rostec corporation and the entities it controls (including RT-Project Technologies and RT-Inform), the Rostelecom national telecom operator and Sberbank are among the largest and most active companies in the Russian ICT sector.

**Rostec** brings together more than 700 companies, mostly from the defence complex, which is Russia's most technologically advanced industry. The companies it controls have been involved in many state-sponsored IT projects in Russia, including the electronic public procurement system and the electronic tolling system for trucks using federal roads. Rostec implemented most of those tasks in cooperation with private subcontractors controlled by members of the Russian political and businesses elite, e.g. the Platon tolling system was developed in collaboration with a company belonging to Igor Rotenberg (the son

<sup>&</sup>lt;sup>10</sup> 'Россия: от цифровизации к цифровой экономике', Институт экономики роста им. Столыпина П.А., 14 September 2018, www.stolypin.institute.

of a friend of President Putin), and the tracking system was implemented with a company belonging to Alisher Usmanov (one of Russia's richest entrepreneurs). Companies that form the radio-electronic cluster within Rostec reported the highest turnover among all IT companies in Russia in 2018.<sup>11</sup>

**Rostelecom**, which holds a dominant position in the fixed telecom network and landline internet access became one of the four largest mobile network operators in Russia after taking over Tele2, and is the market leader in the area of data storage and PayTV services. It has also implemented numerous state-sponsored programmes related to the development of IT technology and the digitalisation of the state administration. It provides technology support in such sensitive areas as the election process, e.g. it controls GAS-Vybory – the Russian Federation's automated "Elections" state system. In 2017 Rostelecom became the sole provider of telecommunication services to federal state bodies (it had previously controlled 59% of that market). The Russian Federation's 2019–2021 budget allocates RUB 31 billion to Rostelecom for the development of an integrated telecoms network for the defence, security and law enforcement bodies.

Russia's largest bank, the state-owned **Sberbank**, is also becoming a leading IT company. It has developed its IT segment by acquiring shares in several private companies: in 2015 it acquired majority stakes in Platius (a mobile payments service) and RuTarget (which uses big data to analyse consumer behaviour).<sup>12</sup> It has a staff of more than 45,000 IT workers dealing with its digital business. Currently around 85% of all software used by the bank is developed by companies it controls. Sberbank's IT business also expands beyond the financial sector. In November 2019 the bank started cooperation with Moscow city hall to provide IT services to the inhabitants of Moscow and IT support for the capital's systems for parking, municipal charges, doctor's appointments, school student's grade registers).<sup>13</sup>

In November 2019, Prime Minister Dmitry Medvedev commissioned the creation of a concept to transform the **Skolkovo Innovation Center**<sup>14</sup> into a state-

<sup>&</sup>lt;sup>11</sup> <sup>'</sup>Ранкинг TAdviser100: Крупнейшие ИТ-компании в России 2019', TAdviser, 17 May 2019, www.tadviser.ru.

<sup>&</sup>lt;sup>12</sup> В. Мещеряков, 'Сбербанк купил компанию у основателя Abbyy', CNews, 12 March 2015, www.cnews.ru.

<sup>&</sup>lt;sup>13</sup> Е. Кузнецова, Е. Чернышова, 'Сбербанк переведет сервисы Москвы на свою ИТ-инфраструктуру', РБК, 5 December 2019, www.rbc.ru.

<sup>&</sup>lt;sup>14</sup> An institution in the Moscow area, established in 2010 by then President Dmitry Medvedev and tasked with supporting the development and market rollout of Russian IT solutions. In 2019 it had

-owned integrator tasked with developing and implementing comprehensive IT solutions for state bodies. It would provide all IT services to public bodies (the administration, state-owned corporations, schools, etc.). Private companies, which would lose much of their market share to the state-owned integrator, are opposing the idea. They argue that centralising the services could cause delays in the implementation of the digital economy programme.<sup>15</sup>

Persons with links to the Russian power elite also own companies tasked with, *inter alia*, developing Russian-made technologies. For instance, the non-public **Innopraktika Foundation**, tasked with developing the concept of a 'Silicon Valley' at the Moscow Lomonosov University (the project's value is estimated at RUB 110–120 billion), is controlled by President Putin's daughter Katerina Tikhonova. The largest state-owned companies – including Rosneft, Gazprombank, Rostec and Rosatom – cooperate with the foundation. Its revenues have increased more than two-fold in the years 2014–2018 to RUB 490 million.<sup>16</sup>

In 2016 the Ministry of Economic Development initiated a 'National Champions' programme to support large private high-tech firms. The beneficiaries do not get additional financial assistance but gain direct access to a range of public support instruments, including information and consultancy support in Russia and abroad. Kaspersky Lab is one of the programme's participants.<sup>17</sup>

As demonstrated by the Audit Chamber (the Russian Federation's highest inspectorate), state-owned companies are typically awarded ICT contracts without competitive tenders, by the prime minister's or the president's decision. In most cases, the quoted prices are inflated while the companies usually do not have sufficient human, technological and engineering resources to deliver the contracts and therefore subcontract parts of the work.<sup>18</sup>

more than 250 registered residents and a total of nearly 2,000 start-ups were cooperating with it. For more information see the Skolkovo Innovation Center website at sk.ru.

<sup>&</sup>lt;sup>15</sup> А. Посыпкина, 'Компании предупредили Медведева о риске замедления цифровой экономики', РБК, 16 December 2019, www.rbc.ru.

 <sup>&</sup>lt;sup>16</sup> А. Злобин, 'Фонд «Иннопрактика» Катерины Тихоновой увеличил выручку на 65%', Forbes, 20 November 2019, www.forbes.ru.

<sup>&</sup>lt;sup>17</sup> For more information, see the website of the National Champions programme at www.national--champions.ru.

<sup>&</sup>lt;sup>18</sup> For more information, see: Е. Мереминская, С. Ястребова, 'Счетная палата показала, как зарабатывает на госзакупках структура «Ростеха»', Ведомости, 28 April 2019, www.vedomosti.ru; К. Седов, 'Счетная палата недовольна ходом реализации проекта по созданию электронного правительства', Ведомости, 11 July 2016, www.vedomosti.ru.

The state is the main force promoting the digital transformation in Russia as it has been forcing businesses to implement new technologies, especially in sectors where such technologies can generate new budget revenue, including commerce (online cash registers, automated manufacturing control systems, e.g. in liquor manufacturing, systems to mark and trace goods) and transport (the Glonass satellite navigation system, the Platon tolling system, and navigation seals installed in vehicles). The Stolypin Institute has estimated the burden on Russian business generated by the implementation of obligatory state IT systems at around RUB 80 billion in 2016–2017, of which around 20 billion was the cost of implementing the new duties imposed by the so-called Yarovaya law which forced telecom operators and organisers of information distribution on the Internet (e-mail services, instant messengers and other services that allow messages to be exchanged online) to store the content transmitted (for more information, see Chapter I.3). Mobile operators estimate the cost of complying with the law within the next five years at around RUB 200 billion and have asked the state for support.<sup>19</sup>

#### 3. Subordination of digitalisation to the security agenda

The development of the digital economy in Russia has also been influenced by the authorities' and decision makers' focus on security issues. The Kremlin's priority is to ensure the secure functioning of the system of power in Russia, which is why the Russian security apparatus has had considerable sway over the digital transformation. As those actors view the virtual sphere as a space of quasi-military confrontation, security issues are regarded as more important factors for the development of the digital sector than efficiency or costs.

Since 2012, the Kremlin has taken a series of measures to shield the Russian digital sector from any interference from third countries, and especially the West (by trying to isolate Runet from the World Wide Web, or promoting the use of Russian-made technologies and software), while at the same time tight-ening control of society by restricting online freedoms, especially freedom of speech. The main guidelines in this domain have been laid down in the "Information security doctrine of the Russian Federation", approved by the president in December 2016.<sup>20</sup>

<sup>&</sup>lt;sup>19</sup> Four mobile operators estimate that implementing the Yarovaya law over the next five years will cost around RUB 200 billion. 'Операторы связи попросили у государства денег на исполнение «закона Яровой»', Интерфакс, 29 October 2019, www.interfax.ru.

Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Администрация Президента России, www.kremlin.ru.

The doctrine lists the threats that Russia must counter, including:

- the development, by some Western states, of IT capacities to influence the information infrastructure when pursuing military purposes;
- the rise of technical intelligence targeting Russian government bodies, research organisations and the enterprises of the defence-industrial complex;
- a growing number of digital attacks against critical infrastructure;
- attempts at using information and psychological tools with a view to destabilising the internal political and social situation in various regions across the world, undertaken by the intelligence services of numerous states in order to undermine sovereignty and violate the territorial integrity of the targeted states;
- a growing number of foreign media publications that offer biased assessments of the state policy of the Russian Federation; growing information pressure on the population of Russia, primarily on Russian youth, with the aim of eroding Russian traditional spiritual and moral values; discrimination against the Russian media abroad and obstacles faced by Russian foreign correspondents;
- the high dependence of the Russian industry on foreign IT (electronic components, software, computers and telecommunications);
- the low efficiency of Russian research institutions working to develop prospective information technologies; the low efficiency of efforts to roll out the relatively few Russian-made technological solutions that exist;
- a rise in cybercrime, primarily in the financial sphere;
- the fact that some states exploit their technological superiority to dominate the information space (according to Russia, given the current global distribution of resources required to ensure the safe and steady functioning of the Internet, it is not possible to manage them jointly in a fair and trustbased manner).

The doctrine states that in order to counter those threats, the Russian authorities should increase the resilience of the Russian IT systems to withstand attacks, support the development of domestic technologies and reduce the dependence on foreign providers, and promote patriotism and values rooted in Russian history among the public. Internationally, Russia should be independent in the field of IT and take active measures to ensure the security of the international information system.

To this end, several legal acts have been adopted in recent years. Their provisions include:

- prohibiting internet users in Russia from using tools to circumvent content blocks or conceal the user's identity, such as anonymisation services, VPN networks, proxy servers and TOR networks;
- allowing the Russian government's media inspectorate Roskomnadzor to block access to information and anonymisation services;<sup>21</sup>
- allowing the Russian state bodies to block websites without a court order this applies not only to websites offering indisputably harmful content (e.g. child pornography, the promotion of drug use and the encouragement of suicide), but also to those which publish criticism of the government. A 'black list' of banned website has been created;
- the creation of barriers to the online publication of content, e.g. by requiring popular bloggers to meet requirements applicable to media companies;
- requiring legal persons to store the personal data of Russian citizens only on servers located in the territory of Russia;
- forcing communications service providers, owners of Internet resources and messenger apps to store all the content (e.g. transmitted text and audio-visual data, as well as recordings of phone calls and text messages) for six months and to make them available to the secret services without a court order; require messaging apps to disclose encryption keys at the request of the Federal Security Service (FSB) (this requirement comes from the Yarovaya law named after Irina Yarovaya, one of the authors of the regulation);

<sup>&</sup>lt;sup>21</sup> Putin for the fourth time. The state of and prospects for Russia (2018–2024), OSW, Warszawa 2018, www.osw.waw.pl.

- abolishing the anonymity of instant messaging (IM) users and requiring the disclosure of a unique customer number;
- prohibiting the dissemination of fake news that poses a threat to "the health or life of citizens or which creates the risk of mass public order or security disruption", as well as information that "offends public morals and human dignity and expresses disrespect for society, the state, state symbols, the constitution or the state authorities of the Russian Federation";<sup>22</sup>
- aiming to build a 'sovereign internet' in Russia, i.e. infrastructure that could support the continued functioning of the Russian internet (Runet), should it be cut off from foreign servers. The authors of this idea point to the risk of hostile action on the part of the United States. In reality, the aim is for the government to take control of Runet. A centralised governmental management system for online communications in Russia is going to be created in the event of threats to the security of Runet, complete with internet exchange points and cross-border data transmission. Internet service providers will be required to install "technical measures of security threat detection" on their network connections, to provide state bodies with extensive information about how they use the web infrastructure, the addresses served, data transmission routes, internet exchange points and the cross-border network. They will also be required to cooperate with law enforcement bodies in testing internet security in Russia. The law calls for minimising cross-border traffic in communication between Russian users. Moreover, by the end of 2020 a national domain name system is going to be created, independent of the global DNS system managed by the US-based ICANN. Some of the law's provisions entered into force already in November 2019.23

The measures to ensure internet security have mainly served the purpose of combatting the opposition in Russia, while efforts to counter terrorism and online crime have been much less effective. According to the Russian Prosecutor's Office, the number of criminal acts involving the use of modern technologies has increased more than six-fold in the years 2013–2016, and in 2017 increased by a further 30% (compared to 2016). The Prosecutor's Office reports that more than 180,000 cases of cybercrime were registered in 2019,

<sup>&</sup>lt;sup>22</sup> M. Domańska, J. Rogoża, 'Russia: stricter Internet censorship', OSW, 13 March 2019, www.osw.waw.pl.

<sup>&</sup>lt;sup>23</sup> M. Domańska, 'The Runet fortress: the Kremlin's struggle with the 'hostile' internet', OSW, 19 April 2019, www.osw.waw.pl.

i.e. nearly 67% more than in 2018, the most frequent type of this crime consists in the fraudulent use of banking cards.<sup>24</sup> The Association of Lawyers of Russia estimates that Russia loses around US\$ 2 billion a year as a result of cybercrime.

#### 4. The regulatory framework of the digital transformation

The need to build a digital economy in Russian has been spelt out in various Russian legal acts over the last two years. First, the process was announced in the "Strategy for the development of the information society in the Russian Federation in the years 2017-2030", approved by a presidential decree on 9 May 2017.<sup>25</sup> Its main directions were described then in the governmental programme "Digital economy of the Russian Federation", adopted on 28 July 2017 as an implementing document of the presidential decree.<sup>26</sup> The programme's objectives and timelines of activities in different areas were laid down in more detail in sectoral action plans developed in late 2017 and early 2018, for example for the development of information infrastructure or the provision of information security. The digital transformation earned its special status – as well as access to public funds – after the president recognised the **development of the digital economy** as one of the thirteen strategic national programmes. The programmes are expected to put Russia on a dynamic development path by 2024 (i.e. by the end of Vladimir Putin's fourth term), as stated in the presidential decree of 8 May 2018.<sup>27</sup>

There are numerous legal documents that mention the digital transformation, but they only offer a very general definition of the digital economy. The governmental programme contains a brief explanation, stating that in the digital economy "the digital version of data is a key means of production in all spheres of the society and economy, increasing the economy's competitiveness and the citizens' quality of life, promoting economic growth and the state's sovereignty".

<sup>&</sup>lt;sup>24</sup> В. Шмырова, 'Киберпреступность в России растет быстрее любых других видов преступлений', CNews, 27 September 2019, www.cnews.ru.

Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», Администрация Президента России, www.kremlin.ru.

<sup>&</sup>lt;sup>26</sup> 'Об утверждении программы «Цифровая экономика Российской Федерации»', Правительство России, 31 July 2017, www.government.ru.

Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», Администрация Президента России, www.kremlin.ru.

The documents do contain detailed descriptions of the specific objectives that the government aims to achieve by 2024 thanks to the implementation of the digital economy national programme. The programme itself has been divided into six parallel projects.

#### State projects implementing the digital economy in Russia

- The **"Human Resources"** project aims to educate a qualified workforce for the digital economy; from 2024, at least 120,000 IT specialists are expected to graduate from Russian universities and enter the job market each year.
- The **"Information Security"** project aims to ensure security in Russia, e.g. by deploying Russian-made software and technologies for the transmission, processing and storage of data to guarantee the protection of personal data and the interests of business and the state. By 2024, 97% of internet users and 90% of state and local government bodies in Russia are expected to use information protection software, most of which should be Russian-made.
- The "**New Technologies**" project aims for state-of-the-art technologies to be developed by Russian specialists and using Russian research. By 2024, research and development funding for areas such as big data, blockchain, artificial intelligence, quantum technologies and robotics is expected to increase by 300%. Public and private spending on the development of the digital economy is expected to increase from 1.7% of GDP in 2017 to 5.1% in 2024.
- The **"Digital Public Administration"** project deals with the implementation of digital technologies and platforms to support the decision-making process in the public administration and to facilitate the provision of services to the public and business. By 2024, 70% of all contacts with the public administration are to take place online, and all services provided by the state and local administration are to be available without the need for an in-person visit.
- The **"Information and Communication Infrastructure"** project aims to create a global, competitive infrastructure for the transmission, processing and storage of data, based mainly on Russian-made

technologies and software. This includes: the implementation of 5G standards, the development of the Internet of Things (IoT), and the provision of broadband internet to the public. By 2024, 97% of house-holds and all public institutions are expected to have access to broadband internet, and Russia's share in the global data storage market is set to increase to 5%; by 2021 5G mobile networks are expected to be implemented in ten cities with populations above 1 million.

• The **"Legal Regulation"** project envisages the creation of the necessary legal framework to comprehensively regulate the development of the functioning of the digital economy in Russia.

# 5. Selected actors involved in the "Digital Economy" national programme

In January 2020, a series of reshuffles in the Russian government resulted in the replacement of most persons hitherto responsible for the implementation of the "Digital Economy" programme (see below for details). An analysis of the changes suggests that the Kremlin decided to change the way the sector is governed. The original model based on young technocrats coming from the digital sector and having no political backing turned out to be ineffective, leading to delays in the implementation of the programme.

Before January 2020, most officials in charge of the ICT sphere and formally authorised to formulate Russia's digital economy policies were younger generation politicians (until 21 January 2020, Maxim Akimov, born in 1970, was the deputy prime minister for digital transformation, and Konstantin Noskov, born in 1978, was the minister for the digital transformation). Both were regarded as technocratic, efficient managers and enthusiasts of the digital transformation, but they had no cadres or political backing of their own and were political lightweights in the governmental administration. They also had no effective influence on the decisions regarding the most important orientations of the sector's development, such as the investment climate or the security--related aspects.

In January 2020, the responsibility for the digital transformation was transferred to a new set of people who have close links to the IT sector but not necessarily degrees in the subject, and who have successfully implemented digitisation projects for the public administration and have good relations

18

with important members of the Russian political and business elite. With this background, they will likely be able to deliver on their tasks in keeping with the logic and needs of the Russian elite in a situation where – while the digital transformation is a priority for the government – its implementation has been subordinated to Russia's national security objectives. In this setting, experts in charge of the technical side of the digital transformation have often faced resistance from the security apparatus or businesses, and have had to give up on solutions that would be technologically optimal. This has created the risk that the cost of the transformation may increase, and suboptimal concepts may be selected for implementation. Nevertheless, the new leaders of the governmental programme may be much more willing to accommodate the expectations of the security agencies.

A separate category of officials holding important positions related to communications and the mass media comprises people with military backgrounds, probably with links to military intelligence (e.g. the deputy minister for digital transformation Oleg Ivanov, or Alexander Chechin, deputy chief of Roskomnadzor; see below for more information), who have a direct influence on the sectors of communications and the media. Functionaries of the FSB and other secret services seconded to the public administration bodies also have a say in the decision making on the digital transformation. Their role in the government of the Russian Federation is expected to increase following the recent reshuffles.

#### The most important persons and bodies involved in Russia's digital transformation currently include:

- **Prime Minister Mikhail Mishustin** (born 1966). He took office on 16 January 2020 and owes his nomination largely to positive opinions about his performances as the chief of the Federal Tax Service. The successful digitisation of the service's resources considerably improved its efficiency. Mishustin was also in charge of the digitisation of Russia's cadastre. His mission is to accelerate and efficiently implement all the national programmes that are the pillars of President Putin's economic policy. However, given Mishustin's background and the fact that the "Digital Economy" programme is the most delayed, he will probably pay special attention to it.
- Deputy Prime Minister for Transport, Communication and Digital Technologies Alexei Overchuk (born 1964). Appointed on 21 January 2020, he replaced Maxim Akimov. Overchuk graduated from the Agrarian

University in Moscow where he studied economic cybernetics and is regarded as an efficient manager. A long-time aide of Prime Minister Mishustin. The two men have worked together on the successful digitisation of Russia's cadastre and the tax system. Most likely he will be the prime minister's close aide in charge of the digital transformation. His duties include coordinating the implementation of the "Digital Economy" national programme.

The Ministry of Digital Development, Communications and Mass • Media of the Russian Federation (the Ministry for Digital Transfor**mation)**. It is in charge of formulating policies and proposing regulations in the fields of IT, telecommunications (including the use and release of radio frequency bands), mass communications and the mass media (including electronic media) and the development of internet, television and radio broadcasting (including digital), implementation of new technologies, the processing of personal data and other domains. Since 21 January 2020, Maxut Shadayev (born 1979) has been at its helm, having replaced Konstantin Noskov. Shadayev previously worked at the state-owned Rostelecom, where he was deputy CEO since 2018. He graduated from the State Social University of the Ministry of Labour and Social Development (currently the Russian State Social University, RSSU) and is a sociologist by education. He has sat on the management boards of several IT companies. Since 2004, he has held positions in state administration structures: in the Ministry of Information Technology in the years 2004–2008, then as information society advisor to Sergey Naryshkin, head of the Presidential Administration (of the then President Dmitry Medvedev) and a close aide of President Putin's with a background in the special services. In 2012 Shadayev followed Naryshkin to work for the State Duma (he advised on the digitisation of the parliament's resources). In the years 2014–2018 he was the Moscow Oblast's Minister for Digitisation. Press reports suggest that since 2017 he has also advised Sergey Kiriyenko, head of the internal policy division in the Presidential Administration (of President Putin). An analysis of Shadayev's career suggests that he has links to the secret services.

Since July 2018, **Evgeny Kislyakov** has served as first deputy minister for the digital transformation and has been responsible for administering the "Digital Economy" programme. Kislyakov graduated from the Moscow Aviation Institute (MAI) where he studied economics and has held various positions in the government since 2003. In August 2018 **Oleg Ivanov**, a radio electronics engineer who transferred to the ministry from Roskomnadzor, was appointed as a deputy minister.

- The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) is a body under the Ministry for Digital Development. It oversees compliance with the legislation on communications, information technology and the media, as well as personal data protection. The service is also authorised to take measures related to the use of radio frequencies and controls the General Radio Frequency Centre. In March 2020 Andrei Lipov (born 1969) was appointed chief of Roskomnadzor. He previously worked in the Presidential Administration where he coordinated work on the draft law on sovereign internet. Together with Lipov, Alexander Terlyakov and Vladimir Logunov also moved from the Presidential Administration to Roskomnadzor where they took the posts of deputy chiefs. Another deputy chief post has since 2019 been occupied by Alexander Chechin (born 1963), a retired lieutenant colonel of the Armed Forces of the Russian Federation. Previously, Roskomnadzor had for eight years been overseen by Alexander Zharov (born 1964) whom independent commentators and the opposition consider to be a dutiful Runet censor. Several opposition portals have been blocked as a result of Roskomnadzor's measures.
- The "Digital Economy" Autonomous Non-commercial Organisation (ANO) was established by the sector's largest state-owned and private companies including Rostec, Rosatom, Rostelecom, VTB Bank, Yandex, Mail.ru, mobile operators, and the Russian government. It plays an important role in Russia's digital transformation as a platform for consultation between business and the state. For example, it formulates objectives and drafts analyses and other documents. Evgeny Kovnir (born 1973), the ANO's CEO since 2017, is a governmental bureaucrat and IT specialist with a military background who graduated from the Kyiv Suvorov Military School, the Zhukovsky Air Force Engineering Academy in Moscow, and the Russian University of Economics. Under the previous government (of Dmitry Medvedev) business representatives tried to use the organisation to lobby their interests and block unfavourable solutions proposed by the government; this considerably prolonged the consultation processes. With the current composition of the government, the ANO's influence on the digital transformation process may diminish and business is likely to become more subordinated to the state's policies.
- **The state telecom company Rostelecom** (see Chapter I.2). Nearly 49% of Rostelecom shares are held by the state treasury while the state-owned development corporation VEB holds another 4% and Mobitel (a Rostelecom

subsidiary) holds a 15% stake. The remaining shares are traded in exchange markets. Rostelecom's board of directors is chaired by Sergei Ivanov (former deputy prime minister and defence minister, former secretary of the Security Council of the Russian Federation, former chief of the Presidential Administration and a trusted aide of President Putin, whom Ivanov has known since the 1970s when they both worked in the KGB). Rostelecom is mostly active in the fixed telecommunications sector and only entered the mobile sector a few years ago with the takeover of the Tele2 telecom company. As of April 2019, Rostelecom held 45% of shares in Tele2, the remainder being held by the state-owned bank VTB (27.5%), the oligarch Alexei Mordashov (a close collaborator of Igor Sechin) who owns 22%, and Rossiya Bank (controlled by President Putin's friends including Yuri Kovalchuk) - the bank holds a 5.5% stake. An assets consolidation process is currently underway, as a result of which the original shareholders of Tele2 will become shareholders in Rostelecom. However, state-owned entities will continue to control the company.

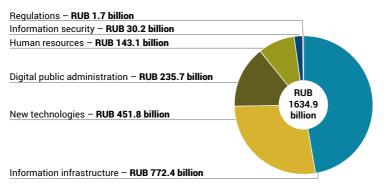
The Rostec state corporation (see Chapter I.2) controls approximately 700 enterprises from different sectors of the economy, mostly the defence industry. It is also in charge of the development of Russian IT technologies and software and for identifying and supporting promising projects. It works on the implementation of blockchain technology in Russia and on expanding data collection, storage and processing capacities. Its CEO Sergei Chemezov is a former close acquaintance and aide of President Putin with a background in the special services.

#### 6. Financing the "Digital Economy" programme

Many details of the implementation of Russia's digital transformation are unclear and therefore the estimates of its total cost are only indicative. In accordance with the materials published by the government in February 2019,<sup>28</sup> the "Digital Economy" national programme has been allocated financing of around RUB 1.6 billion (around US\$ 26 billion, based on the January 2020 exchange rate) in the years 2018–2024, most of which (around RUB 1.1 billion) will come from the federal budget with the remainder provided by other sources, mostly business. The expansion of information infrastructure will be the most expensive part of the programme and will consume around half of the budget.

<sup>&</sup>lt;sup>28</sup> Национальные проекты: целевые показатели и основные результаты, Правительство России, 7 February 2019, www.government.ru.

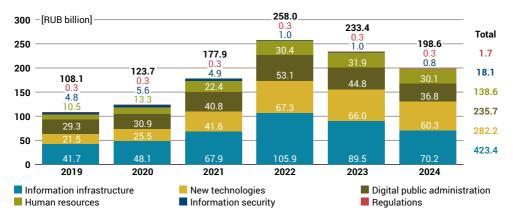
**Chart 1.** Estimated total cost of the "Digital Economy" national programme in the years 2018–2024



Source: Национальные проекты: целевые показатели и основные результаты, ор.cit.

According to the Russian Accounts Chamber, in 2019 the "Digital Economy" programme's implementation was the slowest among all thirteen national programmes. Its 2019 budget was RUB 108 billion, but only 8% of the total was spent during the first six months of 2019, and throughout the year only 73% of the sum was spent, corresponding to around RUB 79 billion (half of it in December). That was the total value of signed contracts and agreements for state subsidies.<sup>29</sup>

**Chart 2.** Federal budget spending on the "Digital Economy" national programme, broken down into the six projects



Source: Budget of the "Digital Economy" national programme for the years 2019-2024.<sup>30</sup>

- 29 Е. Кинякина, С. Ястребова, '«Цифровая экономика» потратила пятую часть годового бюджета за три дня', Ведомости, 13 January 2020, www.vedomosti.ru.
- <sup>30</sup> Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации», Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 30 June 2019, www.digital.gov.ru.

One of the reasons why the programme is so delayed concerns the need to develop and adopt new regulations as this requires a lot of consultation, including direct talks with business. The "Digital Economy" programme provides that businesses from the digital sector will be an equal partner in the programme's implementation, hence consultations are crucial.<sup>31</sup>

The low level of spending is also linked to the funding's 'toxic' nature. Government officials and entrepreneurs alike fear taking decisions and using the public funds because of several systemic factors including the instability and ambiguity of regulations, centralised and non-transparent decision-making processes, and politically motivated and selective anti-corruption measures that mainly reflect feuds between the different security agencies. Large stateowned corporations with links to the ruling elite are in principle the only category of businesses that apply for the funds. They are not able to deliver on the contracts themselves, but the terms they offer to subcontractors (low rates, delayed payments, defaults on payments) have been discouraging private businesses from co-operating. As a result, the volume of unspent funding in the federal budget has increased threefold in the last three years (in 2019, unspent funds were reported at around RUB 1 billion, i.e. more than 5% of total budget spending).

<sup>31</sup> Я. Милюкова, И. Юзбекова, 'Токсичные деньги: почему за выполнение майского указа Путина можно получить 20 лет', Forbes, 3 October 2019, www.forbes.ru.

#### II. RUSSIA'S 5G NETWORK DEVELOPMENT PLANS

Development of the information infrastructure, and especially the creation of the 5G mobile network, is the cornerstone of Russia's digital transformation programme. All official documents that deal with the digital economy foresee the growth of 5G technology in Russia. Replacing the 4G (LTE) standard with new generation technology will considerably increase data transmission speeds (up to 20 Gb/s for downloading and up to 10 Gb/s for uploading), minimise lags (to 4 ms at most, which can be further reduced to 1 ms), and enable the connection of a much larger number of devices (up to 1 million devices per 1 square kilometre). The implementation of 5G technology is expected to revolutionise wireless communication and spur further the automation and digitisation of business processes.

The development of 5G networks is advanced in many parts of the world – South Korea is one of the global leaders when it comes to implementing the standard. In April 2019 three South Korean mobile operators launched commercial 5G networks using the 3.5 GHz and 28 GHz frequencies, and Samsung has put 5G compatible smartphones on the market.

Russia has been trying to join the global trends in mobile communications development. Russian operators are currently testing new solutions in cooperation with multinational companies (in particular, Ericsson, Nokia and Huawei). At the same time the Russian government is working on legislation to regulate the development of 5G technology. The efforts to implement the 5G network in Russia offer a perfect illustration of the wider problems that the Russian state will face while implementing the entire digital transformation programme.

#### 1. The current state of the mobile market in Russia

According to analyses by the TMT Consulting agency, in 2019 the Russian telecoms market was worth RUB 1.73 billion (around US\$ 28 billion based on January 2020 exchange rates). Its revenues had grown 2.1% compared to 2018, which means growth has been slower (the year before revenues had grown 3.4% year on year). Mobile communications account for the largest share of the market (55%), followed by internet access provision (12%) and fixed phone services (8%). The fastest growth in recent years was reported in the Pay-TV sector (more than 10% year on year in 2018) and mobile communications (more than 5% year on year). The market for commercial data storage and processing services has also been growing dynamically in Russia in connection with the security requirements imposed on operators. Unlike most states, however, Russia does not have any standards for the operation of these facilities. As a result, it is not possible to objectively assess the quality of their services or the capacity of data storage servers.<sup>32</sup>

In 2019, the largest mobile operators (the 'big four') accounted for 99% of the mobile sector's total revenues and of the total number of customers (data as of end of June 2019): $^{33}$ 

- **MTS**, Russia's largest operator, had a market share of 30%. MTS is a private corporation registered in Russia. AFK Sistema, a company controlled by the oligarch Vladimir Yevtushenkov,<sup>34</sup> holds a majority stake in the company and the remaining shares are traded in exchange markets, including outside Russia. The company provides services to 78.1 million mobile users in Russia and more than 20 million in the former Soviet states.
- MegaFon accounts for slightly less than 30% of the market. Its largest shareholder is the USM Group controlled by one of Russia's wealthiest oligarchs Alisher Usmanov (USM Group holds 56.32% of its shares).<sup>35</sup> Other shareholders include Gazprombank Group (18.79%) and MegaFon Investment Ltd., a subsidiary of MegaFon registered in Cyprus (3.92%). The remaining shares are traded in markets. The company provides services to around 75.9 million users in Russia. MegaFon's technical infrastructure is also used by Yota, a mobile virtual network operator.
- **VimpelCom** and its brand Beeline account for 21% of the market. Vimpel-Com is part of the international group VEON Ltd. The company currently provides services to around 54.3 million users in Russia and more than 180 million outside Russia. Its main shareholders include Letter One,
- <sup>32</sup> Российский рынок телекоммуникаций: предварительные итоги 2017 г., ТМТ Консалтинг, December 2019, www.tmt-consulting.ru.
- <sup>33</sup> 'Cellular Data 2019', Advanced Communications and Media, www.acm-consulting.com.
- <sup>34</sup> In recent years Vladimir Yevtushenkov has fallen victim to the growing business ambitions of Igor Sechin, one of the most powerful members of the Kremlin power elite. Yevtushenkov has lost his stake in the Bashneft oil company and his control of MTS also hangs in the balance. For now, he has managed to keep control of this mobile operator, but the Kremlin has many instruments at its disposal to change its ownership structure at any moment.
- <sup>35</sup> Alisher Usmanov is a Kremlin-dependent oligarch, his main assets are concentrated in the extractive and metallurgic industries and in recent years his involvement in the IT sector has also been growing. Among other assets, he holds shares in the Mail.ru group, which is currently developing its own communicator known as TamTam.

a company owned by Russian oligarchs Mikhail Fridman, German Khan and Alexei Kuzmichev (47.9%), Norway's Telenor (19.7%) and the Netherlands' Stichting Administratiekantoor Mobile Telecommunications Investor (8.3%).

• The state-owned **Rostelecom**, which has taken over the mobile operator Tele2, accounts for 18% of the market (around 45.9 million mobile users in Russia). It has reported the fastest growth in market share, at 2 percentage points in two years (for more information on Rostelecom, see Chapter I.6).

#### 2. The development of the 4G network in Russia

All the 'big four' operators have been involved in the development of the 4G network in Russia. Under the terms of their licences to provide this standard of service, awarded in 2012, each of them was required to invest at least RUB 15 billion a year in the development of infrastructure.

As of early December 2019, Russia had 324,000 4G base transceiver stations (the number increased by 13% in the course of last year). The 'big four' offered 4G services in all 85 regions, mostly in the capital cities, and in some cases also in smaller cities. 4G access was available mainly in central Russia.<sup>36</sup> In February 2018 (the most recent study available) OpenSignal estimated access to LTE in Russia at 65% (compared to 59.1% in June 2017),<sup>37</sup> and average download connection speed at 15.77 Mb/s (compared to 16.6 Mb/s in June 2017).

In 2019 VimpelCom/Beeline expanded its network of base transceiver stations at the fastest rate (a 50% increase), but it still has the smallest number of LTE stations among the 'big four' (65,400). Tele2 also reported rapid expansion (by 46%) and currently has the second-largest number of 4G stations (more than 75,700). MegaFon's network of 4G stations is still the largest in Russia – in early December 2019 the operator had more than 107,400 LTE stations (having added 23%). MTS had the third-largest network with 75,500 stations (21% more than the year before).<sup>38</sup> Initially, Russian operators relied on the technological solutions offered by European companies such as Ericsson and Nokia to develop their networks, but in recent years Huawei has increasingly become the preferred option. All Russian operators are making efforts not to

<sup>&</sup>lt;sup>36</sup> Mobile network coverage maps for Russia: www.4gltee.ru/zona-pokrytiya-v-rossii.

<sup>&</sup>lt;sup>37</sup> OpenSignal does not study the geographical coverage of 4G, but the proportion of time when users of 4G-compatible devices are within range of the LTE network: 'The State of LTE (February 2018)', Opensignal, www.opensignal.com.

<sup>&</sup>lt;sup>38</sup> Roskomnadzor's communiqué, VK, 26 December 2019, www.vk.com.

become dependent on a single supplier and to cooperate with different partners. Ericsson's technologies are still the most popular solution in the Russian market, followed by Huawei, Nokia, Samsung and ZTE (see Appendix 2 for more information).

The LTE licences authorised the operators to use lower frequency bands (including 720–790 MHz, recognised by the State Commission for Radio Frequencies as prospective for the development of LTE in 2011, and 791–862 MHz) as well as the 2.50-2.69 GHz band. Moreover, they also developed 4G networks using frequency bands allocated to the lower standards, i.e. 2G (900 MHz, 1800 MHz) and 3G (2100 MHz).<sup>39</sup>

Band (according to the 3GPP classification)	Radio frequency (MHz)	Technology
Band 3	1800-1880	FDD (Frequency Division Duplex)
Band 7	2620-2690	FDD
Band 20	790-820	FDD
Band 31	450	FDD
Band 38	2570-2620	TDD (Time Division Duplex)

Table 1. Radio frequencies for the 4G network in Russia

Source: 'Какие частоты 4G у российских операторов — Полный обзор', 4G connect, 7 May 2018, www.4gconnect.ru.

Lower frequency bands below 1 GHz are occupied by the Ministry of Defence, the Ministry of Industry and Trade, the Federal Air Transport Agency or Rosaviatsiya (for radar navigation and radiolocation, etc.), as well as television operators. Mobile operators were expected to gain access to lower frequencies upon completion, in 2019, of television's shift to digital broadcasting as this

39 В. Кодачигов, 'Операторы нашли частотам для 3G и GSM новое применение', Ведомости, 5 February 2019, www.vedomosti.ru.

was expected to free up some frequencies. However, after the 700 MHz band was distributed among mobile operators through tenders in 2012, digital television broadcasters took steps to gain access to those frequencies as well, claiming that the 470–694 MHz band allocated to them was insufficient, especially in view of the development of HD technologies. The lobbying efforts by television broadcasters were successful. Among these were efforts by President Putin's friends, such as Yuri Kovalchuk, who controls one of Russia's largest media holdings, the National Media Group. In August 2014 the president sided with the broadcasters, issuing a decree which banned making frequencies reserved for television available "for other purposes" without the consent of the television broadcasters.<sup>40</sup> Mobile operators have so far failed to obtain such consent.

By the end of 2019, digital terrestrial television (DDT) in Russia had launched two multiplexes (works are underway to launch more), which can broadcast on frequencies between 470 and 862 MHz. Depending on the region, digital television stations use various bands, including in the 700 MHz range.<sup>41</sup> However, to avoid interfering with the LTE networks that use 800 MHz, they do not use frequencies above 790 MHz.

The other users of bands below 1 GHz, especially the Ministry of Defence and Rosaviatsiya, have also succeeded in delaying their re-allocation. Initially, in 2014, neither body objected to the shift, but wanted to carry it out on their own. They asked for funds from the federal budget for this purpose, effectively blocking the Ministry of Communications from taking over control of the process. Within the framework of the federal programme, "Modernisation of the single air traffic organisation system in the years 2009–2020", Rosaviatsiya has replaced some of the old airport radar systems that use frequencies below 1 GHz (DRL-7SM) with new systems that operate above 1 GHz (AORL). However, around 40 old systems were still in operation in 2019.

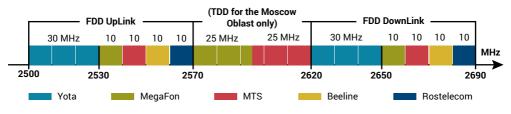
As a result, mobile operators have not been able to use the 700 MHz range. Moreover, they have faced serious constraints in accessing the 791-862 MHz frequencies officially allocated to them for the purposes of developing the LTE Advanced standard. Their access to the 880-960 MHz band (allocated

Указ Президента Российской Федерации от 11.08.2014 г. № 561 «О гарантиях распространения телеканалов и радиоканалов на территории Российской Федерации», Администрация Президента России, www.kremlin.ru.

<sup>&</sup>lt;sup>41</sup> Interactive map of digital terrestrial television transmitters with transmission frequencies: 'Интерактивная карта ЦЭТВ', карта.ртрс.рф.

for the purposes of GSM, 3G, LTE Advanced) was also limited in practice.<sup>42</sup> Local limitations related to the activities of the Ministry of Defence and other actors also apply to access to the 1.8 GHz and 2.1 GHz range of frequencies allocated to the development of the GSM network. Limitations also apply to the 2.3–2.4 GHz frequencies used for mobile communications by the Ministry of Defence and Ministry of the Interior, while local restrictions are sometimes imposed on the 2.50–2.69 GHz range allocated to the LTE Advanced network because the frequencies are also used by aviation radio location systems.<sup>43</sup> Because of these difficulties with the release of lower radio frequencies, the LTE network has mainly been developing in Russia with the use of higher frequencies (see Appendix 1).

**Chart 3.** Frequencies in the 2500 MHz band allocated to mobile operators for the purposes of 4G/LTE



Source: 'Какие частоты 4G у российских операторов — Полный обзор', 4G connect, 7 May 2018, www.4gconnect.ru.

Since 2019, the development of the LTE service for bodies providing important public services (including schools, medical facilities, police stations, fire brigades etc.) in rural areas in Russia has relied on the 450 MHz band.<sup>44</sup> The development of the LTE-450 network is the responsibility of the stateowned companies Rostelecom, the Russian Television and Radio Broadcasting Network (RTRN, the operator of terrestrial radio and television infrastructure in Russia) and Concern Avtomatika, a company owned by Rostec.<sup>45</sup>

The Rostelecom-controlled Tele2 company has had access to the 450 MHz band since 2010 and has been trying to develop LTE-450 on that frequency since 2016. Currently the network operates in several places, including Moscow, Saint Petersburg, and the Moscow and Leningrad Oblasts. Due to its dense coverage,

<sup>42</sup> Awarded as part of the "Концепции создания и развития сетей 5G/IMT-2020 в Р<br/>Ф" project.

<sup>&</sup>lt;sup>43</sup> Л. Коник, '5G-сети в РФ получили план развития', ComNews, 7 November 2018, www.comnews.ru.

<sup>&</sup>lt;sup>44</sup> The 450 MHz band has been used for the purposes of mobile network development in Russia since

the early 1990s. In the 2000s it was used by the CDMA2000 network, a hybrid between 2.5G and 3G. <sup>45</sup> И. Королев, 'Государство потратит 27 миллиардов на 4G-сети для силовиков и спецпотребителей', CNews, 26 March 2019, www.cnews.ru.

LTE-450 is popular among the inhabitants of villages around the two cities and people who have summer homes there. LTE networks using 450 MHz to support important public services will be developed within the "Digital Economy" national programme. The wireless networks using this band will be used primarily by the Interior Ministry, Ministry of Emergency Situations (rescue services) and the National Guard. Moreover, it will also be used to provide broadband internet to providers of important public services.

#### 3. Russia's 5G network development plans

Russia is in the early stages of planning the development of its 5G network. Consultations are underway and numerous disputes concerning crucial aspects of the network are yet to be resolved. As of the end of 2019 it was still unclear what rules would govern the implementation of 5G in Russia.

The preliminary outline of Russia's masterplan for the development of 5G infrastructure was laid down in the governmental programme, "Digital Economy of the Russian Federation"<sup>46</sup> and the **Action plans for the development of information infrastructure** of 18 December 2017, which build and elaborate on the programme. Successive official documents added more detail to the plans or partly amended them. For example the so-called passport of the "Digital Economy" national programme spells out the programme's objectives and timeline, and identifies the official bodies responsible for its implementation.<sup>47</sup>

In accordance with the **timeline** presented in the above documents:

• **by the end of March 2019**, the government was supposed to adopt the crucial document for the development of 5G networks, i.e. the 'concept for the creation and development of the 5G/IMT-2020 in Russia'. In March 2019, the Ministry for Digital Development unveiled the draft document, which received much criticism from business (see Chapter II.5 for more information) and was sent back to the Ministry for further work in March 2020. At that point consultations and lobbying started to change some of its provisions. As a result, the concept has still not been adopted by the government;

<sup>&</sup>lt;sup>46</sup> The "Цифровая экономика Российской Федерации" programme was adopted by the government on 28 July 2017, Правительство России, www.government.ru.

<sup>&</sup>lt;sup>47</sup> Паспорт национальной программы утверждён решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 года, Правительство России, www.government.ru.

- **by the end of September 2019**, the State Commission for Radio Frequencies (GKRCh) should have decided what frequency ranges would be allocated to the development of the 5G network in Russia. However, as the security apparatus has been blocking the most useful frequencies, no decision has been made yet. The timeline states that, once the decision on frequencies has been made, by the end of 2020 a plan should be made for the release of the necessary bands for the purposes of 5G;
- **by the end of 2020** pilot projects should be initiated concerning the implementation of the 5G standard in five key sectors in cities with populations of more than 1 million;
- **by the end of 2021** the conditions for the mass implementation of 5G communications are to be defined;
- **by 2024** the 5G network should cover all cities with more than one million inhabitants, and Russian-made technologies should be used for that purpose.

The plans currently in force regarding the development of the 5G network in Russia envisage that the service should initially be available in cities with populations above 1 million (of which there are 15 in Russia) and, as a priority, the services should be made available to selected sectors of the economy. By the end of 2021, the conditions necessary for the launch of the 5G network are to be created in at least ten such cities, and the service is expected to be widely available on a commercial basis as of 2024. This means that the Russian government has extended the deadline for the implementation of the 5G standard by at least one year compared to the initial plans and has reduced the number of cities where the service is to be implemented (the original plan was for all cities with over million inhabitants to be covered). The then Minister for Digital Development Konstantin Noskov explained that the delays had been due to insufficient commercial demand for the technology in Russia and difficulties with identifying the frequencies on which it should operate.

According to the government, the 5G network should serve primarily to support industrial projects and selected sectors, and a fragmentary network should be sufficient for the cities. The choice of sectors that will be offered 5G service will be made on the basis of a profitability and demand analysis. It is believed that the 5G network may be particularly useful in transport and

should be developed along transport corridors. However, the necessary analyses have not been conducted yet.<sup>48</sup>

Deputy Prime Minister Maxim Akimov, who was previously responsible for the digital transformation programme, confirmed in a conversation with President Putin in April 2019 that the implementation of the 5G network in Russia would start in 2022 and take at least ten years. According to his estimates, it will cost around RUB 650 billion (which in early 2019 corresponded to US\$ 10 billion). He also announced that the Russian government would make every effort to ensure that a considerable portion of the budget goes to Russian companies, and not multinational telecom corporations such as Cisco, Huawei, Ericsson and Nokia. Contracts with potential foreign providers of technology and equipment will include clauses requiring such companies to locate manufacturing in Russia.

An important assumption for the development of the 5G network, and for the entire digital transformation agenda, is that the process should be implemented using Russian technologies, software and devices. In April 2019, the Ministry of Industry and Trade presented a draft target programme for the development of industrial production for the fifth-generation network and the IoT in the Russian Federation in 2019–2024.<sup>49</sup> The draft programme allocates around RUB 28 billion (ca. US\$ 0.5 billion), of this some 60% from the federal budget, to supporting the development of Russian-made devices and software for the purposes of the 5G network and the IoT. Its implementation will involve Rostec and the Skolkovo Innovation Center as well as companies from the sector whose products are listed in the register of Russian-made telecom devices.<sup>50</sup> Those include RDP.RU (a company in which Rostelecom has held shares since 2016), the Novosibirsk-based private company Eltex, the Ufa-based NPP Poligon (with links to the former deputy prime minister of Bashkortostan Dmitry Sharonov), NPF Mikran (under US sanctions since 2016); the private company T8 (which co-operates closely with Rostelecom). The programme will

<sup>&</sup>lt;sup>48</sup> Decision of the working group for the digital transformation of September 2017. The 2017 documents envisaged that by the end of 2020 all federal roads should be covered by communications networks enabling wireless data transmission. In 2018 the group suggested that mobile communications and wireless data networks should not only be developed along roads, but also around all transport infrastructures including rail and aviation facilities. The plan was to develop hybrid networks using satellite and mobile technologies.

<sup>&</sup>lt;sup>49</sup> The document has not been published, but the Russian media has seen a copy. М. Коломыченко, 'Власти направят F28 млрд на разработку криптостойкого оборудования для 5G', PBK, 26 April 2019, www.rbc.ru.

<sup>&</sup>lt;sup>50</sup> An entry in the register, kept by the Ministry of Industry and Trade of the Russian Federation, is a kind of certificate attesting that a product or software is made in Russia. The register is available here: www.minpromtorg.gov.ru/opendata.

co-finance research and development, and the deployment and the manufacture of micro and macro components for different kinds of telecom networks. It will also subsidise manufacturing for businesses from Russia and the Eurasian Economic Union, and partly also for foreign customers. The ministry expects that in 2022, the share of Russian-made devices and software in the Russian 5G and IoT networks will reach 16% and grow further to 19% by 2024.

The Ministry of Digital Development adopted a **Concept for the development** of the IoT in early April 2019.<sup>51</sup> The document had been drafted by a working group operating under the "Digital Economy" ANO with the support of the Ministry of Transport and the Federal Security Service. The concept envisages, for instance, the creation of a register of IoT identifiers to recognise and identify the users of all networks and to *de facto* create a closed IoT network in Russia. The network is then supposed to be connected to the FSB's System for Operative Investigative Activities (SORM), the Service's IT system that monitors telephone and internet communications in Russia. While many issues important for the implementation of the 5G standard in Russia remain unresolved, in July 2020 Roskomnadzor granted MTS the first licence for the development of the 5G network in 83 Russian regions using the 24.25–24.65 GHz frequencies. The licence is valid for five years. The service will be available to MTS's business customers and industrial plants.<sup>52</sup>

#### 4. 5G network testing

The lack of clarity about the future rules for the 5G network have not stopped Russia's mobile operators from investing in related technologies and implementing pilot projects. Those projects will serve as a basis to formulate the rules and conditions for the mass implementation of 5G communication and the entire network development concept. Before 2018, the tests used the 3.4–3.8 GHz and 25.25–29.5 GHz bands. They were conducted by two operators only: the state owned Rostelecom and the private MegaFon. MTS and Vimpel-Com were denied access to the frequencies because of negative opinions issued by the security forces.

In summer 2016 MegaFon became the first operator in Russia to obtain GKRCh's permission to test 5G technologies. It was possible because the company *de facto* 

<sup>&</sup>lt;sup>51</sup> The document has not been published. И. Королев, 'Власти создают в России суверенный интернет вещей', CNews, 4 April 2019, www.cnews.ru.

<sup>&</sup>lt;sup>52</sup> 'МТС получила первую 5G лицензию в России', MTS press service, 28 July 2020, moskva.mts.ru.

acted as a subcontractor of the state-owned company Rostec. MegaFon was allowed to carry out tests on the 3.4–3.8 GHz and 25.25–29.5 GHz bands in all 11 cities in which the 2018 World Cup games were organised. The Russian operator carried out tests on the 3.4–3.8 GHz band in cooperation with China's Huawei (under a cooperation agreement signed by the companies in 2014), and on higher frequencies (a 400 MHz-wide channel in the 28 GHz band) in cooperation with Qualcomm Technologies Inc. and Nokia. In May 2018 MegaFon and Nokia signed a memorandum on strategic cooperation in the implementation of the 5G network and digital technologies.

In January 2018 GKRCh also authorised companies of the Freshtel group (owned by Rostelecom) to carry out 5G tests on the 3.4–3.6 GHz frequencies. The companies cooperated on projects with Ericsson, Huawei and Nokia (and others).<sup>53</sup>

The most recent tests on the 3.4–3.8 GHz band conducted by Rostelecom and MegaFon ended in December 2018. In April 2019, GKRCh yielded to pressure from the security sector and suspended any further testing on those frequencies. At the same time GKRCh awarded all four mobile operators access to the 4.8–4.99 GHz and 25.25–27.5 GHz bands for the purposes of pilot tests in several large cities in Russia.

VimpelCom signed an agreement with Ericsson in 2018 concerning the development of the 5G network and the IoT in 2018–2020. In August 2019 it signed a three-year strategic cooperation agreement with Russia's OVRPOWER (Metrocom S.A.) to work on virtual reality (VR) and augmented reality (AR) in 5G networks.

In June 2019, MTS signed an agreement on joint 5G tests in Russia in 2019–2020 with Huawei. A similar agreement has also been signed with Ericsson. MTS is also involved in cooperation with Russian entities, including the Skolkovo Innovation Center, with which it aims to conduct research and development into solutions for the 5G standard (including open radio access network architecture, Open RAN). Moreover, MTS and MegaFon are going to test the 5G network in Saint Petersburg on the 2.5–2.7 GHz frequency to which they have access due to tenders won in 2015.

<sup>&</sup>lt;sup>53</sup> Freshtel tested the 5G standard in the Saint Petersburg Hermitage Museum using Ericsson devices, in Innopolis (a special technology zone in Tatarstan) in cooperation with China's Huawei, and at the Skolkovo special zone in cooperation with Nokia.

# 5. Works on the 'concept for the creation and development of the 5G/IMT-2020 network in Russia'

In accordance with the adopted documents concerning the development of the digital economy in Russia, **the 'concept for the creation and development of the 5G/IMT-2020 networks in Russia'** was supposed to be approved by the end of March 2019. Two weeks before the deadline, the Ministry for Digital Development sent a draft document to the other ministries for consultation. The draft was heavily criticised, and no consensus could be reached despite nearly one year of debating. In December 2019, the Ministry for Digital Development adopted the document in a version fiercely opposed by the mobile operators. As a result, after the government reshuffles in March 2020, the draft was sent back to the ministry for further elaboration. The two crucial issues that remain unresolved concern:

- **access to radio frequencies**: the ANO "Digital Economy", network operators and the Federal AntiMonopoly Service (FAS) are calling for the network to be developed on the radio frequencies which are globally recognised as optimal, including 3.4–3.8 GHz, and for those ranges to be made available as soon as possible by their current users, i.e. mainly the Russian security apparatus. They are also demanding access to the 694–790 MHz frequencies (the so-called 700 MHz band) to expand coverage, especially along transport routes. However, the security agencies are unwilling to release the 3.4–3.8 GHz frequencies and suggest the network should be developed on the 4.8–4.99 GHz range. Furthermore, television broadcasters are unwilling to free up the 700 MHz band;
- **the network operator model**: the Ministry of Digital Development and Rostelecom have been calling for the creation of a single 5G infrastructure operator, while private companies and the FAS have argued that the network should be shared by operators. In December 2019, the Ministry for Digital Development forced the four operators to create a consortium to deal with the release of radio frequencies. The state is currently demanding a stake in the newly created company.
- **5.1.** The vision of the 5G network as proposed by the Ministry for Digital Development

The 'concept for the creation and development of the 5G/IMT-2020 network in Russia' drafted by the ministry is largely based on studies by the Radio Scientific Research Institute (NIIR).

### The draft looks at **three scenarios for the implementation of the 5G net-work in Russia**:

- each of the four operators develops its network independently while sharing the infrastructure e.g. masts, sites, optical fibre (some 10–15% of infrastructure is shared);
- intensive/extensive network sharing (some 50-70% of the infrastructure is shared);
- **3.** the network is developed by a single infrastructure operator.

The draft envisages that the 5G network will be implemented by 2024 in the 15 cities with populations above one million, with special focus on business centres, residential areas and industrial zones within the cities, and along transport corridors. The draft concept states that, in order to comprehensively provide access to 5G/IMT-2020 services in Russia, it is necessary to comply with the conclusions of the 2015 and 2019 World Radiocommunication Conferences (WRC-15 and WRC-19) on access to various radio frequency ranges including the 694-790 MHz, 3.4-3.8 GHz and 24.25-29.5 GHz bands. The draft also recalls that the tests already carried out have confirmed the usefulness of those frequencies for the development of the 5G network. It identifies access to the 3.4–3.8 GHz band as a priority but – in view of the deficit of available frequencies (only 80 MHz of bandwidth is currently available) – it suggests that initially, the 4.4-4.5 GHz and 4.8-4.99 GHz bands regarded as auxiliary (they offer a bandwidth of up to 100 MHz) should be used. Within the range of 24.25–29.5 GHz, each operator, including the single infrastructure operator, should gain access to a bandwidth of 400 MHz. A clear statement on the use of the 700 MHz range appears only in the corrected version of the draft concept, prepared by the Ministry for Digital Development in April 2020. The document also states that, in order to improve the efficiency and speed of 5G/IMT-2020 network implementation, it will be necessary to also use the radio frequencies allocated to lower-generation mobile networks (2G, 3G, 4G).

The Ministry for Digital Development argues that the best option for Russia would be to implement the third scenario, in which a single infrastructure operator develops the 5G network. It would reduce the cost that the operators will have to incur to build and operate the network, guarantee the fastest rate of project implementation and non-discriminatory access to resources. The shortage of available radio frequencies in the 1–6 GHz range has also been

quoted as an argument in favour of the third scenario because a single operator could work with a narrower bandwidth than four independent operators. In the single operator scenario, the total investment needed to develop 5G infrastructure to 2024 would be around RUB 55 billion, while the development of the network by each operator separately would cost three times as much.

In late 2019 the Ministry of Digital Development forced the private operators to form a consortium for the purposes of developing the 5G/IMT-2020 network in Russia. Its main task is to deal with the release of the radio frequencies: 700 MHz, 3.4–3.8 GHz, 4.4–4.99 GHz and 24.25–29.5 GHz. The consortium agreement was signed on 11 December 2019. Before that happened, the ministry threatened that if the operators refused to sign it, they would not be given free-of-charge access to the 4.4–4.9 GHz band, as previously planned. However, it has since turned out that the operators and the ministry have different views on how the consortium should work. From the point of view of the companies, the consortium was not supposed to be a mobile operator itself. Each member would have equal rights to use the allocated frequencies, select regions for operation and co-decide on the terms on which the shared 5G infrastructure would be developed. This would allow them to preserve at least partial competition.

However, the ministry, already with Shadayev at the helm, informed the operators in January 2020 that establishing a single infrastructure operator was still the government's priority and only in that case could they count on obtaining frequency allocations free of charge. The revised draft of the concept unveiled in April also included a new demand from the ministry, which now wants to control the consortium created by the operators and acquire a stake in it.

## **5.2.** Criticisms of the draft concept for the development of the 5G network

The conclusions of the studies by the Radio Scientific Research Institute differ from the results of analyses by the private Spectrum Management consultancy<sup>54</sup> which, in the autumn of 2018, prepared an **alternative draft concept for the creation and development of the 5G network in Russia**, commissioned by the LTE Union (an association of Russian LTE operators).

In June 2018 the Spectrum Management company lost the tender for the development of the 5G network development concept organised by the ministry (which Radio Scientific Research Institute won). The company was founded in 2016 by Olga Gubanova, who controls 100% of its shares.

The alternative concept argues that the optimum solution would be to develop the 5G network using new frequencies (694-790 MHz, 3.4-3.8 GHz and 24.25–29.5 GHz) and those already in use (for 2G, 3G and 4G), with the four operators extensively sharing communications infrastructure (as in the second scenario).<sup>55</sup> Spectrum's draft concept was based on studies conducted by the international consultancy firm PricewaterhouseCoopers (PwC) published in a May 2018 report. The report concluded that the most efficient and least expensive formula would be for infrastructure to be built in a competitive setting, jointly by two or more operators (i.e. with extensive infrastructure sharing). PwC estimates that in that scenario, the cost of network development in the years 2020-2027 would amount to around RUB 550-610 billion (US\$ 7.5-8.5 billion) and would correspond to around 8% of the entire mobile sector's annual revenues. The option where all operators develop their own infrastructures would be the costliest. The option of a single national infrastructure operator developing the network, on the other hand, would be the most time-consuming option and one with the highest service costs once the network becomes operational (because of the absence of competition). The PwC study also showed that the increase in mobile network coverage in Russia achieved as a result of the development of the 5G standard to 2027 (provided that the necessary radio frequencies are allocated) would not be more than 20% compared to the lower generation networks. In the most probable scenario, coverage would increase by a mere 4–10%<sup>56</sup> (for a comparison of the assumptions of both concepts, see Table 2).

Both the businesses and the ANO "Digital Economy" have expressed positive views of the Spectrum draft and have criticised the studies of NIIR. The ANO "Digital Economy" called into question the credibility of NIIR's analysis of the cost of the three scenarios, especially in view of the possibility that it might be necessary to use frequencies other than those applied worldwide.

The provisions of the governmental draft concept for the development of the 5G network were also criticised by Russian manufacturers and sellers of electronics, and IT companies who argued that the proposed state support for domestic companies was insufficient and that their interests would not be adequately protected.

<sup>&</sup>lt;sup>55</sup> А. Устинова, 'Отрасль выступила против концепции инфраструктурного оператора 5G', Com-News, 15 April 2019, www.comnews.ru.

<sup>56</sup> в России. Перспективы, подходы к развитию стандарта и сетей, PricewaterhouseCoopers, May 2018, www.pwc.ru.

In May 2019, the ministry's draft was also criticised by the FAS. It stated that the establishment of a single 5G network operator and allocating radio frequencies exclusively to that operator would lead to the monopolisation of the network. That, in turn, could lead to higher prices and a lower quality of service. In this option, the state would also forgo potential revenue from tenders for access to radio frequencies (below 6 GHz). Moreover, the FAS argues that if a single operator is created, this could cause problems with using the 4G infrastructure (owned by private operators) for the 5G network if the operators do not join the consortium forming the single operator. As a consequence, the implementation of the 5G standard could be slowed down and the sector would stagnate. The FAS also notes that if Russia decides to build the 5G network using frequencies different from those employed by most countries, that could cause connectivity problems in the border areas and lead to a shortage or higher prices of 5G compatible user devices.<sup>57</sup>

**Table 2.** Estimated cost of the development of the 5G network in Russia (RUB billion)\*

	Scenario 1 Separate networks of four operators	Scenario 2 Extensively shared network	Scenario 3 Single infrastructure operator		
according to the Radio Scientific Research Institute					
In all 15 cities with populations above 1 million in 2020–2024	161	113	56		
of this, in Moscow	41	29	16		
according to Spectrum Management					
In all large cities in 2020–2027	550-610	400-445	330-365		
* The estimated cost of acquiring imported devices is based on an exchange rate of US\$ 1 = RUB 70.					

<sup>7</sup> П. Белавин, В. Новый, Д. Шестоперов, '5G предлагают разделить на всех', Коммерсантъ, 23 May 2019, www.kommersant.ru.

As a result of the ongoing disputes, the 'concept for the creation and development of the 5G/IMT-2020 network in Russia' has still not been adopted by the government. In the autumn of 2019, the Ministry for Digital Development tasked the Radio Scientific Research Institute with preparing a new study to plan the conversion of radio frequencies for the purposes of the 5G/IMT-2020 network. The aim of the study was to once again identify the bands that would be used for this purpose, the cities where the implementation of 5G would be economically viable, a cost estimate of the conversion process, and the potential sources of financing.<sup>58</sup> According to press reports, the ministry officials overseeing the preparation of the plan refused to accept the document delivered due to its low quality, and in January 2020 they were dismissed.<sup>59</sup> No information is available on what happened next with the study. The proposed conversion plan has not been published.

### 6. The dispute over radio frequencies for the 5G network

**6.1.** The main new radio frequency bands necessary for the development of 5G networks

To ensure the stable development of the 5G network, operators need to have access to the frequencies already in use for the lower generation mobile networks (2G/3G/4G) and to new frequencies:

• **below 1 GHz**: those frequencies are crucial for overcoming physical obstacles (hills, walls, large distances). They enable large area coverage to be built and are useful especially for network development in the provinces. The signal from transmitters using frequencies below 1 GHz, including the 694–790 MHz band, reaches far distances and may extend even 200–300 kilometres beyond state borders. Therefore, to avoid interference, it is crucial to harmonise the use of frequencies for the purposes of 5G between neighbouring states (at the international level). This is why already in 2015, the World Radiocommunications Conference<sup>60</sup> concluded that the **694–790 MHz** band was the most promising. In the aftermath,

<sup>&</sup>lt;sup>58</sup> <sup>(</sup>Минкомсвязь объявила конкурс на подготовку плана по расчистке спектра для 5G', RSpectr.com, 2 August 2019, www.rspectr.com; <sup>(</sup>5G на пороге', RSpectr.com, 5 June 2019, www.rspectr.com.

<sup>&</sup>lt;sup>59</sup> А. Устинова, 'Аппарат ГКРЧ теряет кадры', ComNews, 16 January 2020, www.comnews.ru.

<sup>&</sup>lt;sup>60</sup> The conference is organised by the International Telecommunications Union (ITU) to monitor and set international radio regulations, including agreement on the use of radio frequencies and geostationary and non-geostationary satellite orbits. Russia is an important ITU member. The conferences take place every four years, the most recent one took place in October 2019. For more information, see: World Radiocommunication Conferences (WRC), ITU, www.itu.int.

the European Union imposed an obligation on its member states to release the band for 5G by 22 June 2022 at the latest.<sup>61</sup> Russia has not made a similar decision yet even though **all documents adopted so far point to the** 700 MHz band as necessary for the functioning of the 5G infrastructure and suggest that its current users should be transferred to lower frequencies. It is also assumed that each operator will need a bandwidth of 5-20 MHz in this range;

- **1-6 GHz**: those frequencies make it possible for the network to simultaneously serve a large number of connected devices. This range of frequencies may be successfully used in large, densely built-up cities. The WRC-15 and WRC-19 guidelines state that the **3.4-3.8 GHz** band and, complementarily, the **4.4-4.99 GHz** band are of priority importance for the development of 5G. Moreover, all the documents pertaining to the implementation of 5G in Russia assume that the **3.4-3.8** GHz band will be the main frequency range and the **4.4-4.99** GHz will be auxiliary.<sup>62</sup> In 2019, however, the Russian security forces started to block access to the **3.4-3.8** GHz band for mobile operators, suggesting that in the initial phases, the network could be developed using the **4.4-4.99** GHz frequencies. The draft concept for the creation and development of the 5G network provides that each operator should be allocated 50 MHz of bandwidth within this range. Therefore, the total bandwidth needed is 200 MHz, or 190 MHz in the case of a single operator;
- **above 6 GHz**: those frequencies offer high speed data transmission but are effective within short distances only; the proposed band is **24.25-29.5 GHz**. Tests in Russia have been conducted mainly for the **25.25-27.5 GHz** band; operators are expected to apply for 400 MHz of bandwidth each. This range is currently fairly busy and would need to be released by its current users. The plan is to move the ground stations of the terrestrial-satellite communication network which use the 24.25-27.5 GHz outside big cities. There have been objections to those plans.

One of the main challenges in the implementation of the 5G network in Russia, which posed a problem already in the development of lower-generation

<sup>&</sup>lt;sup>61</sup> Decision (EU) 2017/899 of the European Parliament and of the Council of 17 May 2017 on the use of the 470-790 MHz frequency band in the Union, Official Journal of the European Union L 138, www.eur-lex.europa.eu.

<sup>&</sup>lt;sup>62</sup> For example: План Мероприятий по направлению «Информационная инфраструктура» программы «Цифровая экономика Российской Федерации» of 18 December 2017, Правительство России, www.government.ru.

networks, concerns a shortage of available frequencies. In accordance with the previously adopted timeline, the State Commission for Radio Frequencies had until the end of September 2019 to decide which bands would be allocated for the development of 5G infrastructure. Because of the fierce dispute over this issue, the decision still has not been taken.

#### 6.2. Problems with access to the 700 MHz band in Russia

The 694-790 MHz band in Russia is currently reserved and in use:

- the 694–726 MHz band for transmission of the terrestrial television signal (mainly DTT);
- the 726–790 MHz band for television signal and radio navigation and landing systems.

This frequency range is used by 2,100 transmitters of the two digital television multiplexes functioning in Russia. In the western border areas of Russia, the 700 MHz range is used by just a few transmitters located close to the borders with Norway and Finland (see map). With the current occupancy of frequencies along Russia's western border, no disturbance should be caused to the signal of 5G transmitters in neighbouring countries (assuming that the 5G network in Europe will be built using the 700 MHz band as agreed). However, there is no certainty that in future Russian television stations will not use the range more intensively to implement more multiplexes. The 700 MHz band is also available to regional analogue TV channels that have not joined the two DTT multiplexes. In July 2020 the State Commission for Radio Frequencies extended their right to use this frequency range to 19 August 2021.63 However, it should be remembered that because of problems with maintaining the transmitters, the regional channels increasingly reach their viewers via cable or online TV networks. As a result, the regions often choose to switch off their analogue television transmitters, e.g. the Kaliningrad Oblast completely phased out analogue transmission on 3 June 2019. Under the laws, the band is at the disposal of television broadcasters. Should the Russian multiplexes use the range more, they would interfere with the future 5G networks in countries bordering Russia because the television transmitter signal is much stronger than the signal of mobile networks. This is the reason why it is so important to harmonise decisions on the use of this range between Russia and the EU.

<sup>63</sup> И. Алпатова, 'Без лишних цифр', Российская газета, 13 July 2020, rg.ru.



**Map.** Digital terrestrial television transmitters located close to Russia's borders with countries of the European Economic Area

Digital terrestrial television transmitters located close to Russia's borders with countries of the European Economic Area

Transmitters and frequencies - a selection: Alakurtti: 506 MHz (I), 546 MHz (II) Borisoglebsky: 762 MHz (I), 674 MHz (II) Chernyshevskoye: 602 MHz (I), 586 MHz (II) Elisenvaara: 482 MHz (I), 674 MHz (II) Glubokoye: 514 MHz (I), 594 MHz (II) Yemilovo: 554 MHz (I), 578 MHz (II) Kalevala: 506 MHz (I), 602 MHz (II) Kaliningrad: 682 MHz (I), 586 MHz (II) Kalinino: 602 MHz (I), 586 MHz (II) Kingisepp: 546 MHz (I), 562 MHz (II) Kostomuksha: 482 MHz (I), 570 MHz (II) Kovdor: 474 MHz (I), 618 MHz (II) Krasnogorodskoye: 554 MHz (I), 578 MHz (II) Krasnoznamensk: 602 MHz (I), 586 MHz (II) Lendery: 530 MHz (I), 562 MHz (II) Mamonovo: 682 MHz (I), 586 MHz (II) Naystenyarvi: 722 MHz (I), 594 MHz (II) Nikel: 762 MHz (I), 674 MHz (II) Nikolshchina (Lavry): 698 MHz (I), 754 MHz (II) Ostrov: 554 MHz (I), 578 MHz (II) St. Petersburg: 586 MHz (I), 666 MHz (II) Pechenga: 762 MHz (I), 674 MHz (II) Puykkola: 482 MHz (I), 674 MHz (II) Rayakoski: 474 MHz (I), 666 MHz (II) Reboly: 530 MHz (I), 562 MHz (II) Ruskeala: 482 MHz (I), 674 MHz (II) Sebezh: 514 MHz (I), 594 MHz (II) Slantsy: 546 MHz (I), 562 MHz (II) Sofporog: 482 MHz (I), 514 MHz (II) Sortavala: 482 MHz (I), 674 MHz (II) Sovetsk: 602 MHz (I), 586 MHz (II) Svetogorsk: 498 MHz (I), 722 MHz (II) Trutnevo: 498 MHz (I), 514 MHz (II) Vaulino (Pskov): 698 MHz (I), 754 MHz (II) Vyartsilya: 722 MHz (I), 594 MHz (II) Verkhnetulomsky: 490 MHz (I), 658 MHz (II) Veselovka: 602 MHz (I), 586 MHz (II) Vyborg: 498 MHz (I), 722 MHz (II) Zapolyarny: 762 MHz (I), 674 MHz (II) Zarechensk: 594 MHz (I), 530 MHz (II) Zheleznodorozhny: 682 MHz (I), 586 MHz (II)

Digital terrestrial television transmitters emitting a signal in the 694–790 MHz band and their frequencies are marked in red.

The number of the Russian Television and Radio Broadcasting Network (RTRN) multiplex is given in parentheses.

Borders of frequency zones in the Russian Federation are marked with a dotted line.

Source: Interactive map of digital terrestrial television transmitters with transmission frequencies: 'Интерактивная карта ЦЭТВ', карта.pтpc.pф.

Until the 700 MHz range is reserved for the development of the Russian 5G network and freed by its current users (especially DTT), the development of 5G networks in neighbouring European countries, including **Poland, will face difficulties.** The Ministry of Digital Development estimates that converting the Russian terrestrial television stations to lower frequencies would cost around RUB 1.5 billion (around US\$ 25 million). The broadcasters have yet to present a clear position on this. They have previously suggested that they will need the frequencies in question to broadcast an HD signal. The current position of the broadcasters on the 700 MHz range is expressed in the draft 'concept for the development of radio and television in 2020–2025' which they have prepared and which has been seen by the Russian media.<sup>64</sup> In the document, they declare that they would be willing to make part of the 694-790 MHz band available for 5G (while maintaining control of most of it) on the condition that the process is financed by mobile operators. For now, no information is available on which frequencies would be released, or when and in what form the document will be adopted.

The conversion of radionavigation and landing systems, on the other hand, is underway. Most of those installations are owned by the Ministry of Defence and Rosaviatsiya. The systems, installed at 130 airfields and onboard 1,300 aircraft, are being moved to higher frequencies (960 MHz). However, the process is facing many difficulties, is costly, and will take a long time – it is not expected to be completed before 2028.<sup>65</sup>

It should also be noted that in tenders organised in 2012, all four mobile operators were allocated frequencies from the 720–790 MHz range (each operator receiving two 10 MHz bands) and the 791–862 MHz range (two 7.5 MHz bands) for the purposes of LTE development (see Chart 4). However, they have not been able to use the frequencies because of resistance from television broadcasters and the military. The current users of those frequencies will presumably also be unwilling to swiftly free them for 5G infrastructure.

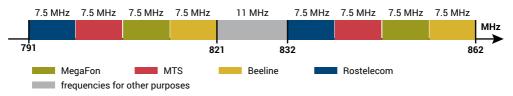
The Russian authorities are in no hurry to unblock the 700 MHz band, especially since there is no plan to develop the 5G network outside large cities in the initial phase. The range would be useful in ensuring the availability of 5G service along transport routes, though. For their part, the mobile operators

<sup>&</sup>lt;sup>64</sup> А. Скрынникова, Е. Ефимович, С. Соболев, А. Балашова, 'ТВ-вещатели назвали условия для передачи своих частот под 5G', РБК, 10 September 2020.

<sup>65</sup> В. Савицкий, 'Лакомые радиочастоты не раньше 2028 г.', ComNews, 30 May 2016, www.comnews.ru.

have not been pressuring the authorities to resolve the matter and have focused on obtaining access to the 3.4–3.8 GHz frequencies.

**Chart 4.** Frequency bands in the 800 MHz range allocated to mobile operators for 4G/LTE network



Source: 'Какие частоты 4G у российских операторов — Полный обзор', 4G connect, 7 May 2018, www.4gconnect.ru.

6.3. Limitations on access to the 3.4–3.8 GHz band in Russia

The 3.4–3.8 GHz frequencies are almost fully occupied in Russia. They are used mainly by radio communication systems, microwave transmission and satellite communication infrastructure, most of which belong to the Ministry of Defence and the Federal Protective Service (FSO). Specifically, that includes:

- radiolocation systems: military air defence systems (3.2–3.8 GHz) with around 1,000 stations including 600 on land and 400 onboard aircraft;
- satellite signal control (3.4–3.45 GHz frequencies used by the Russian Satellite Communications Company); satellite transponders including those transmitting federal television channels (3.45–3.8 GHz);<sup>66</sup>
- radio communication, including base stations providing fixed wireless access (FWA), Wireless Local Loop systems, Fixed Broadband Wireless Access, WiMAX. Until 11 March 2021, the FWA stations will continue to be controlled by two mobile operators: Rostelecom and MegaFon.<sup>67</sup>

The 4.4–4.99 GHz band is much less occupied, especially in large cities in Russia. The 4.4–4.5 GHz and 4.8–4.99 GHz bands are used by the stations of micro-

<sup>&</sup>lt;sup>66</sup> И. Королев, 'Российские 5G в опасности: Власти выделили им самые маргинальные частоты', CNews, 15 April 2019, www.cnews.ru.

<sup>&</sup>lt;sup>67</sup> Rostelecom controls FWA stations via the Freshtel group and its companies: Progress, Orion, Interproject and Stolitsa. MegaFon owns the Neosprint and Neosprint Spb companies. Государственная Комиссия по Радиочастотам при Министерстве информационных технологий и связи Российской Федерации, решение от 10 марта 2011 года N 11-11-05 «Об использовании радиоэлектронными средствами фиксированного беспроводного доступа полос радиочастот 3400-3450 МГц и 3500-3550 МГц», Кодекс, www.cntd.ru.

wave transmission links, and the 4.5–4.8 GHz band by satellite ground stations (space to earth). In December 2018, the State Commission for Radio Frequencies announced that a 190 MHz band in the 4.8–4.99 GHz range was free and could be used for the 5G network.

Before the end of 2018, all plans for the development of the 5G network in Russia, including those prepared by the Ministry for Digital Development and the companies from the sector, assumed that 3.4–3.8 GHz would be the network's basic band, with the 4.4–4.99 GHz in an auxiliary role.<sup>68</sup> The operators were testing the 3.4–3.8 GHz frequencies and preparations (ordered by the ministry) were underway to move the current users to other frequencies or move their transmitters outside large cities so that they do not disturb the operation of the 5G network. Deputy Prime Minister Akimov in 2019 even announced that the state was prepared to finance the freeing of radio frequencies for the 5G network. In 2018 mobile operators estimated the cost of the process at RUB 15 billion, i.e. around US\$ 300 million.<sup>69</sup>

Reports that the security agencies were unwilling to free the 3.4–3.8 GHz range emerged only in late 2018. In March 2019, the Ministry of Defence expressed its objections in its opinion on the draft 5G development concept presented by the Ministry of Digital Development. According to the Defence Ministry, transferring the band to mobile operators would be premature. Moreover, at its request, 5G tests using those frequencies in Russian cities have been suspended. The security forces have stepped up efforts to promote the idea of initially implementing 5G in Russia using the 4.4–4.99 GHz band. Representatives of those institutions were not convinced by the arguments raised by mobile industry experts who argued that the tests already carried out had demonstrated the usefulness of the 3.4–3.8 GHz bands. The same experts also pointed out that Russia could face a deficit of technologies and devices compatible with 5G operating on higher frequencies, leading to much higher prices since global technology companies have been focusing their research on developing 5G networks on the 3.4–3.8 GHz band and mass-produced equipment will be compatible with those frequencies. The likelihood of interference with the Russian 5G network operating on the 4.8–4.99 GHz frequencies in the border areas has also been raised because NATO's air force radiolocation systems actively use the band.70

<sup>68</sup> For example, План Мероприятий..., op. cit.

<sup>&</sup>lt;sup>69</sup> С. Ястребова, 'Государство оплатит расчистку частот для 5G', Ведомости, 30 January 2019, www.vedomosti.ru.

<sup>&</sup>lt;sup>70</sup> В. Кодачигов, Е. Кинякина, 'Совет безопасности снова отказался отдавать операторам частоты для 5G', Ведомости, 14 May 2020, www.vedomosti.ru.

In April 2019 Deputy Prime Minister Akimov asked President Putin to intervene with regard to the negative position of the Ministry of Defence. However, despite his previous declarations about the high priority of the digital economy and 5G implementation, Putin decided that the dispute should be resolved by the Security Council of the Russian Federation, which is dominated by the security apparatus. By doing so, he effectively sided with the Ministry of Defence. In the summer of 2019, the Security Council reaffirmed the Defence Ministry's negative opinion on releasing the 3.4–3.8 GHz band for the purposes of 5G implementation,<sup>71</sup> and in May 2020 once again rejected the operators' requests to release the band in the largest cities in Russia.

Using frequencies from the 3.4–3.8 GHz band currently allocated to the mobile operators Rostelecom and MegaFon for FWA services could be a partial solution to the problem. In 2021, their licences for those frequencies will expire, which offers another argument for them to be repurposed. Both companies are willing to do so and, in the autumn of 2018, they even created a consortium to develop 5G infrastructure using those frequencies. However, for now Rostelecom and MegaFon have not been able to obtain permission from the security apparatus. Moreover, the available bandwidth would not be sufficient.

In all probability, the Russian state-owned companies involved in the development of technologies and devices for the 5G standard are also involved in lobbying for the 3.4–3.8 GHz frequencies. Most of them, for example Rostec, are part of the defence and security complex. This transpires from the statement by Yury Borisov, the deputy prime minister responsible for the defence and security complex, who in September 2019 announced a possible way out of the impasse and that the security force would partially free the 3.4–3.6 GHz frequencies in cities. However, the process would not be on a large scale<sup>72</sup> and no official decisions to this effect have been taken to date.

<sup>&</sup>lt;sup>71</sup> С. Ястребова, 'Путин не отдает операторам популярные частоты для 5G', Ведомости, 14 August 2019, www.vedomosti.ru.

<sup>&</sup>lt;sup>72</sup> See the interview with Deputy Prime Minister Yury Borisov: 'Вице-премьер Юрий Борисов: «Ситуация на космодроме «Восточный» нас не устраивает»', Ведомости, 1 September 2019, www.vedomosti.ru.

#### III. PROSPECTS OF RUSSIA'S DIGITAL TRANSFORMATION AND CONCLUSIONS

The actions taken so far to implement the "Digital Economy" programme in Russia, and especially to develop the 5G mobile network, indicate that the Kremlin is genuinely willing to finance the undertaking and involve industry partners in its implementation. However, several issues raise doubt about whether the digital transformation can accomplish its ambitious objectives.

Firstly, **the contradictory interests of the various actors involved have been causing delays and diminishing the efficiency of the digital trans-formation**. The Russian government's priority is to keep control of the whole process and the emerging new sector of the economy, which they see as a way to ensure Russia's security. As a result, economic efficiency and the speed of implementation of the digital transformation have become subordinated to security issues. The Kremlin has taken various measures to protect the Russian digital sector from interference from third countries, especially Western states (by boosting the autonomy of the Russian internet or promoting the use of Russian-made technologies and devices). However, the objective of technological development in Russia is to tighten control of the public by restricting online freedoms, especially the freedom of speech. As a consequence, the security apparatus, whose main concern is security rather than economic development and modernisation, have gained considerable influence on the digital transformation and the development of the digital economy.

For the companies associated with the Russian ruling elite, the digital transformation is primarily a way to gain access to public funds. The opaque mechanisms for the distribution of public funds offer opportunities for financial abuse and the siphoning off of public funds to private pockets. Even at the current early stage it is already clear that a large proportion of public contracts are being awarded to selected state-owned companies managed by people with links to the ruling elite, and are awarded not through tenders, but rather by the president's or the prime minister's decision. Moreover, the state-owned companies in question are usually unable to deliver on the contracts on their own and subcontract the work. The experience so far shows that the subcontractors are not adequately remunerated, and in many cases do not receive payment at all. As a result, the efficiency of the funds spent is very low, project implementation is often delayed, and the costs are increasing. In such conditions, private technology firms and mobile operators, who care about competition and profits, are not interested in investing in the digital economy in Russia. The "Digital Economy" national programme reported one of the slowest rates of implementation among all the thirteen national programmes underway in Russia. According to preliminary estimates of the Ministry of Finance, 73.8% of the funds allocated to the programme have been used, corresponding to RUB 73.3 billion (this is the value of contracts signed).

Several factors have contributed to the programme's difficulties. The delays are due to ongoing disputes about the very concept of the development of the digital economy (including disputes within the government), which mean the implementation cannot begin in many areas. The slow spending of available public funding, on the other hand, is related to the funds' 'toxicity'. Officials and private businesses alike are wary about taking decisions and spending public funds because of such systemic problems as instability and the ambiguity of regulations, the centralisation and non-transparency of decision-making, and also because of politically motivated, selective anti-corruption measures which mainly reflect feuds involving the security apparatus.

Secondly, **Russia's current economic model considerably diminishes the efficiency of the digital transformation**. Following established logic, the Russian elite seeks to monopolise the ICT sector as well. Until recently, it developed in Russia in a largely competitive setting involving the four mobile operators. As a result, most people in Russia now have access to affordable broadband internet and the range of mobile coverage was systematically expanding, and the software market and e-commerce have been developing dynamically.

For the last several years, though, the Russian leadership has viewed the digital sector as an area of a quasi-military confrontation. Consequently, the state has tightened control of it, as evidenced by the strong position of state-owned companies (Rostec, Rosatom) there. The government has also been increasingly positive about the plans to create a 'sovereign' internet, i.e. a centralised state system for the governance of online communications in the Russian Federation, including internet exchange points and cross-border data transmission. In relation to the development of the 5G network, this tendency has manifested itself in the establishment's preference of a single infrastructure operator. The state takeover of the digital sector has diminished its efficiency and inflated its costs. It has also discouraged private business from investing its capital in the process, although it had been intended that this would play an important role. All this means that it may be difficult to achieve one of the principal aims of the digital transformation, that is to make the digital sector a new driver of economic growth in Russia.

Thirdly, a rivalry continues between the various state institutions for position within the structure of power in Russia. This is particularly visible in the disputes over access to radio frequencies for the purposes of 5G development. The Ministry of Defence has resisted calls to free the necessary frequencies, not only due to state security concerns and technical limitations, but primarily in order to demonstrate its strong position. The ministry had previously been unwilling to allow the unblocking of frequencies for the needs of the 3G and 4G infrastructure, which were released only after an intervention by then President Medvedev and without compromising the security of Russia. The current tough stance of the Ministry of Defence is probably also part of the power games among the Russian security apparatus seeking to obtain high funding from the state budget. A change of their approach, especially to the radio frequencies issue, will largely depend on whether President Putin becomes directly involved in the process.

Moreover, the shortage of Russian technologies will be a serious barrier for the Russian digital transformation. According to the governmental plans, the implementation of the digital economy should rely on Russian--made technologies. Given the scale of Russia's current dependence on foreign suppliers - especially of electronic hardware - achieving this objective will be very difficult and costly. In May 2020, Russian mobile operators pointed out that the requirement to use only Russian-made technologies would considerably delay the implementation of the 5G network in Russia, making it impossible for the network to become operational by 2024.<sup>73</sup> Most of the public financial support for the development of Russian technologies and software ends up in a select group of companies associated with the ruling elite. On top of that, the government plans to halve the funding for the "Digital Economy" programme, including 5G development, in connection with the current crisis in Russia caused by the COVID-19 pandemic and the slump in oil prices.<sup>74</sup> In any case, the Russian state institutions prefer to invest public funds into safe projects for which finance could easily be raised in the market, and are reluctant to become involved in riskier projects that could revolutionise the market in the future in the way Apple or Google have done. In addition, as private IT companies are taken over by state-owned companies, they lose their dynamism, and the bureaucracy and centralised management deprive them of agility. Consequently, more creative IT specialists are choosing to leave Russia.

<sup>&</sup>lt;sup>73</sup> Ю. Степанова, Ю. Тишина, 'По 5G приняли нестандартное решение', Коммерсантъ, 18 June 2020, www.kommersant.ru.

<sup>&</sup>lt;sup>74</sup> Е. Кинякина, 'Пятое поколение связи без денег будет отсталым', Ведомости, 28 May 2020, www.vedomosti.ru.

The government will probably be able to force foreign companies to locate some of their manufacturing plants in Russia, but it is unlikely to become a massive trend or to offer Russia access to state-of-the-art technologies.

Finally, **many of the technological solutions implemented by companies under state contracts turn out to mainly generate burdens on those companies and the public**. The state, which has become the main driver of the digital transformation in Russia, has been pushing for the implementation of systems such as Platon or Glonass, which serve primarily to step up control of business processes or the flow of information. Many of them have imposed additional financial burdens on business without increasing business efficiency. The Stolypin Institute has estimated that the burden imposed on Russian companies by the state-sponsored obligatory digital systems implemented in 2016–2017 cost around RUB 80 billion. Over the next five years, compliance with the requirements imposed by the Yarovaya law will cost mobile operators another RUB 200 billion.

The limiting factors described above have had a particularly negative impact on the development of the 5G mobile network. The programme is already behind schedule and the Kremlin clearly has no intention of accelerating its implementation. The security and revenues of members of the ruling elite seem to be more important in this case than the economic interest of the state.

This is the reason why the government has been refuting the evidence coming from studies, and pushing through the concept of a monopolised market with a single infrastructure operator. In December 2019 the private mobile operators in Russia were forced to create a consortium to build the 5G network and the state is now trying to take over control of it.

As using foreign technologies is inevitable, the Kremlin has been forced to devise adequate safeguards. Moscow does not intend to become dependent on a single supplier and therefore 5G tests have been conducted in cooperation with Ericsson, Huawei and Nokia. At the same time, Russia has been trying to monitor the efforts made by other states, especially in Europe, to ensure the security of their networks. In doing this, it gathers knowledge about experiences that could be useful on its own territory.

The Kremlin's approach to the issue of radio frequencies also suggests that the government is not interested in rapid development of the 5G network in Russia. The security apparatus have been consistently blocking access to the 3.4–3.8 GHz range (without which the development of the 5G network in cities will not only be delayed, but also much more costly), pointing to security concerns. It should be expected that the Kremlin will ultimately decide to free at least a part of this band and allocate it to the national operator. As a result, Russia will develop its 5G network on the frequencies globally recognised as the most useful, i.e. 694–790 MHz, 3.4–3.8 GHz and 24.25–29.5 GHz.

The decision concerning the 694–790 MHz band has been delayed primarily because the final concept of the 5G network in Russia has not been determined yet. Moreover, there are no plans to build the network outside big cities in the initial phase. The band is also less interesting for the operators themselves, because of the low return on investment (among other factors), which is why the operators did not fight hard for access to those frequencies for the purposes of LTE. As the band has a long interference range of up to 200–300 km beyond the borders of a given state, it cannot be ruled out that Russia, which is aware of the approaching deadlines for the releasing of the band set by the EU, has been delaying the process on purpose. In view of the current shape of Russia's relations with the European Union, the Kremlin might want to use the radio frequency issue as a way to pressure Brussels and its EU neighbours. Such a move is likely irrespective of the fact that the digital television stations, to which the band is currently allocated, use it in the border area sporadically.

Following the January 2020 government reshuffle, the digital transformation in Russia will presumably gain a new dynamic. The government will probably be much more willing to compromise and accommodate the demands of the security apparatus to a larger extent than before. The Russian telecom sector will thus have to become ever more subordinated to the centralisation process and Russia's state capitalism model. At the same time, because of the systemic barriers described above and the fact that in 2020 Russia will probably struggle with new serious economic problems caused by the pandemic and the slump in oil prices (which may seriously undermine its financial capacity), no spectacular progress should be expected in the country's digital transformation.

#### IWONA WIŚNIEWSKA

#### APPENDICES

### **Appendix 1.** The LTE network in Russia – division of frequencies among operators

	Operator	Frequencies in MHz (uplink / downlink)	Technology	Band
1.	Yota (MegaFon)	2500-2530 / 2620-2650	FDD	Band 7
2.	MegaFon	2530-2540 / 2650-2660	FDD	Band 7
3.	MegaFon*	2575-2595	TDD	Band 38
4.	MTS	2540-2550 / 2660-2670	FDD	Band 7
5.	MTS*	2595-2615	TDD	Band 38
6.	Beeline	2550-2560 / 2670-2680	FDD	Band 7
7.	Rostelecom/Tele2	2560-2570 / 2680-2690	FDD	Band 7
8.	Rostelecom/Tele2**	832-839.5 / 791-798.5	FDD	Band 20
9.	MTS**	839.5-847 / 798.5-806	FDD	Band 20
10.	MegaFon**	847-854.5 / 806-813.5	FDD	Band 20
11.	Beeline**	854.5-862 / 813.5-821	FDD	Band 20
12.	MTS***	2595-2620	TDD	Band 38
13.	Tele2	453-457.4 / 463-467.4	FDD	Band 31

**OSW REPORT** 10/2020

\* Frequencies allocated for use solely in Moscow and the Moscow Oblast.

\*\* Bandwidth (7.5 MHz) differs from the standard 15 MHz. The operator may use 5 MHz or make an agreement with another operator controlling the adjacent band to combine the bands into one 15 MHz band to be used in the RAN Sharing technology.

\*\*\* Except Moscow, the Moscow Oblast and the Republic of Crimea annexed by Russia.

Source: 'Частотные диапазоны LTE в России', www.anisimoff.org; 'Какие частоты 4G у российских операторов — Полный обзор', 4G connect, 7 May 2018, www.4gconnect.ru.

# **Appendix 2.** Suppliers of devices for the LTE network in Russia (in selected cities\*)

	Operator	City	Frequencies	Device manufacturer	Year of network launch
1.	Yota (MegaFon)	Novosibirsk	2.6 GHz	Huawei	2011
2.	Yota (MegaFon)	Krasnodar	2.6 GHz; 800 MHz	Huawei	2012
3.	Yota (MegaFon)	Moscow	2.6 GHz; 800 MHz; 1.8 GHz	Huawei	2012
4.	Yota (MegaFon)	Sochi	2.6 GHz	Huawei	2012
5.	Yota (MegaFon)	Samara	2.6 GHz	Huawei	2012
6.	Yota (MegaFon)	Vladivostok	2.6 GHz	Huawei	2012
7.	Yota (MegaFon)	Ufa	2.6 GHz; 800 MHz	Huawei	2012
8.	Yota (MegaFon)	Kazan	2.6 GHz	Huawei	2012
9.	Yota (MegaFon)	Kostroma	2.6 GHz	Huawei	2012
10.	Yota (MegaFon)	Tula	2.6 GHz	Huawei	2012
11.	Yota (MegaFon)	Vladimir	2.6 GHz	Huawei	2012
12.	Yota (MegaFon)	Khabarovsk	2.6 GHz	Huawei	2012
13.	Yota (MegaFon)	Orenburg	2.6 GHz	Huawei	2012
14.	Yota (MegaFon)	Krasnoyarsk	2.6 GHz	Huawei	2012
15.	Yota (MegaFon)	Lipetsk	2.6 GHz; 1.8 GHz	Huawei	2013

	Operator	City	Frequencies	Device manufacturer	Year of network launch
16.	MegaFon	Makhachkala	2.6 GHz	Huawei	2014
17.	MTS	Moscow	1.8 GHz; 2.6 GHz	Nokia Siemens Networks (NSN)	2012
18.	MTS	Vladivostok	2.6 GHz; 1.8 GHz	Huawei	2014
19.	MTS	Ekaterinburg	2.6 GHz; 1.8 GHz; 800 MHz	Ericsson	2014
20.	MTS	Ufa	2.6 GHz; 1.8 GHz; 800 MHz	Ericsson	2014
21.	MTS	St. Petersburg	2.6 GHz; 1.8 GHz	Samsung	2014
22.	MTS	Syktyvkar, Vorkuta, Ukhta and others (Komi Republic)	2.6 GHz	Samsung	2014
23.	MTS	Ryazan	2.6 GHz	NSN	2014
24.	MTS	Tver	2.6 GHz	NSN	2014
25.	MTS	Belgorod	2.6 GHz; 1.8 GHz	Samsung	2014

\* Information only about cities where the device manufacturer is known. In most cases the operators do not reveal the device supplier.

**Source:** 'Какие частоты 4G у российских операторов — Полный обзор', 4G connect, 7 May 2018, www.4gconnect.ru.