Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World

Epifanova, Alena; Dietrich, Philipp

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

German Council on Foreign Relations

No. 1
February 2022

DGAP ANALYSIS

Russia's Quest for Digital Sovereignty

Ambitions, Realities, and Its Place in the World

Alena Epifanova
Research Fellow,
International Order and
Democracy Program

Philipp Dietrich
Project Assistant,
International Order and
Democracy Program

Russia's leadership strives for digital sovereignty with two main goals: technological independence and information control. In the face of growing conflicts with "the West" and an ongoing crisis of legitimacy at home, the regime aims to secure its stability by subjugating the IT sector. The consequences of its securitization of the internet and IT market are fatal for innovation and the digital economy. Germany and the EU need to assess their conditional interest in Russia's rapidly changing IT market and communicate their proposals for its regulation.

– **The Russian government does not currently allocate enough resources to digital development to realize its ambitious plans for gaining technology sovereignty.**

– **Although Russia has made considerable progress in internet control in recent years, it cannot yet completely decouple from the global internet and foreign technologies without serious consequences for its people and economy.**

– **Russia heavily depends on Western technologies in its public infrastructure and private sectors. Because this dependence will not vanish anytime soon, it gives Germany and the EU – in coordination with the United States – leverage for both deterring Russia if conflict escalates and continuing to build people-to-people contact between EU and Russian citizens.**

Contents

ACKNOWLEDGEMENTS

The authors wish to thank Tyson Barker, Ansgar Gilster, Madeleine Myatt, Stefan Meister, Milan Nič, and Roderick Parkes for their attentive reviews and valuable comments in support of this DGAP Analysis.

Executive Summary

Over the past decade, Russia has introduced a robust legal framework and numerous regulations meant to shape its future digital sovereignty. In that time, the gap between the Russian state and society has grown and the country is increasingly in a geopolitical conflict with "the West." These two frontlines explain the two main goals in Russia's digital strategy: The regime wants the country to achieve independence in IT and global competitiveness – *technological sovereignty* – and at the same time to gain content security by state control over the internet – *sovereign internet*.

While the digital market in Russia is currently still competitive and diverse, and prospects for developing technology sovereignty in certain areas are bright, the voice of the *siloviki* – Russia's security apparatus – in the digital field has become stronger during recent years. The conflict between the security interests of the Russian state on the one hand and the economic freedom required for innovation and modernization on the other is increasingly visible. The concept of digital sovereignty has been narrowed down by the regime to mean maintaining its stability by subjugating the IT sector.

In recent months, Russia has introduced robust technological means for censorship and demonstrated surprisingly skillful information control on large scales. Yet taking this course to securitization is destroying the conditions for a successful and globally competitive IT sector. The course has already resulted in grievous consequences: several global IT players that were founded in Russia have relocated their headquarters abroad while other home-grown IT champions are being purchased by Western companies. Also, a serious deficit in human resources in the IT sphere could become pressing as a majority of today's IT students want to leave Russia.

To achieve its priority goal of creating a sovereign internet, Russia's government has been actively introducing IT import substitution and fostering protectionism in domestic software and internet services, while simultaneously creating impediments for foreign tech companies. For the time being, however, Russia's economy remains dependent on external – mostly Western – companies and products. Despite the presence of home-grown equivalents to foreign IT provided by Russian firms, there are either not enough or not exclusively domestic solutions to quickly replace the widely used foreign technologies or provide solutions in such key hard- and software sectors as microchip production, 5G solutions, operating systems, and cloud computing. Russia also has very limited power over data that is collected by foreign companies and stored beyond the country's borders. To reach the long-term goal of self-sufficiency in IT, Russia would need to create equivalents for the entire foreign tech stack. This huge challenge is almost impossible to achieve in the short and medium term. Russia's digital and innovation policy is not sufficient to overcome this backlog and achieve genuine technology sovereignty and global competitiveness.

Interestingly, despite ongoing clashes with the West and proclaimed closer cooperation with China, Russia is very reluctant to switch to Chinese alternatives and decouple from proven US and European IT solutions. It has serious security concerns over relying on Chinese IT and understands that, given the United States' tech rivalry with China, negative spillover effects of US sanctions on Chinese companies might recur. While the presumption of Russia's drift toward the Chinese tech sphere has yet to play out, it remains unclear how Russia will balance its tech dependency in the future given the crisis that is currently deepening between Russia and the West.

"Germany and the EU need to be aware of the rapidly changing rules in Russia's IT sector"

Germany and the EU need to be aware of the rapidly changing rules in Russia's IT sector and differences in its understanding of digital sovereignty to a European one. In light of the current geopolitical conflict and ongoing domestic crisis of legitimacy, the importance of the digital sphere will become even greater – possible IT sanctions and technological partnerships, as well as silencing critical voices in Russian society by digital means, will be high priorities for the Kremlin in the years to come.

Germany and the EU need to understand their conditional interest in Russia's digital market and realistically assess possibilities and risks for cooperation with Russian IT companies. Although there are services offered by Russia's internet companies in EU countries, Russia's digital economy is much more interested in US and European tech solutions than the other way around. The coordination of digital policy among EU member states and the United States needs to be improved and could be used as leverage to deter Russia if conflict escalates. Of course, the EU also needs a better understanding of the costs for citizens and the economy on both sides.

At the same time, Germany should use existing fora and involve other EU member states in dialogue with Russia's IT businesses and the government on binding regulations in favor of protecting European companies from the possible risks of Russia's sovereign internet.

Further, when Western countries globally advocate for an open and free internet, as well as the protection of high standards for the digital rights of their citizens from their IT companies, Russian citizens – as users of those technologies – will also profit. Sharper export controls of IT technologies are needed to exclude surveillance and further restriction of freedoms in Russia.

Finally, Russia's society, businesses, and academia are interested in cooperation with Western countries on research in key areas of advanced technologies. The EU should extend its science diplomacy and further engage with Russian universities and scientists in fields of common interest and maintain people-to-people contact between citizens of the EU and Russia.

INTRODUCTION

Russia's push for "digital sovereignty" over the last decade has become one of its most decisive yet overlooked strategic moves. While the definition of the term is kept vague to camouflage the Russian government's desire for greater control over information and its aim to achieve self-sufficiency and global competitiveness in digital technologies, the country's leadership perfectly understands its importance.

The regime of President Vladimir Putin seeks to use digital technologies to secure its future and to establish Russia's role in a changing world order. For the time being, however, Russia remains markedly dependent on external actors, especially the information and communications technology (ICT) of the United States and Europe. Numerous externally owned hardware, software, and social media networks are used in Russia by state authorities, business, and private users.

This dependence on foreign technologies is a vulnerability for the country's leadership, as it sees itself in a conflict on two fronts:

1. With "the West": Indeed, the perception that digital technologies could be weaponized against Russia from abroad has grown in recent years. Since 2014, to evoke fear and justify greater control and IT substitutions, the regime has repeatedly presented a scenario in which Russia finds itself switched-off from the global internet and hit by technological sanctions from the United States, while the country's critical infrastructure is infiltrated by technologically superior states in the West. In that time, the geopolitical conflict between Russia and the West has not only thickened into a crisis, but Russia's concerns have also become real threats. The administration of US President Joe Biden is considering restricting Russia's access to global electronics supplies if Russia invades Ukraine.[1]

2. With its own society: Simultaneously, Putin's regime feels the pressures of self-preservation and seeks to gain the upper hand in controlling all levels of Russian political life. In this context, free internet and the uncontrolled dissemination of critical information are a constant threat. Any real or imagined subversion facilitated by information technologies could jeopardize the system of centralized control over society.

The tension on both these fronts is determining the character of Russia's digital sovereignty strategy and impeding its proclaimed goal of developing its own digital technologies and innovations. To better understand Russia's overall endeavor in digital sovereignty, we suggest differentiating the term into two concepts: *sovereign internet* – content security by achieving state control over all information created and disseminated through the internet within Russia's borders; and *technology sovereignty* – the country's ability to produce its own digital technologies and deploy them for economic growth and international competitiveness without being critically dependent on others.

DIGITAL SOVEREIGNTY IS A HIGHLY CONTESTED CONCEPT

Calls for sovereignty in the digital domain are heard in both authoritarian countries and liberal democracies. Although such calls consist of diverse terminology and foci, they generally concern increasing the role of nation states in internet governance and the development of digital technologies.[2] The particular term **sovereign internet** is a Russian invention that was coined in the last decade during the state's endeavor to control information in the country. **Technology sovereignty**, on the other hand, is a widely used expression that describes a country's intention to develop and use home-grown technologies to avoid one-sided dependency.[3]

Russia is caught in a dilemma. On the one hand, the country needs to develop its digital economy and innovative power to stay competitive with other great powers. On the other, the regime aims to preserve itself and secure its control over society. The existing domestic and foreign policy contradictions are migrating to the digital space.

1 Reuters, "Explainer: The U.S. export rule that hammered Huawei teed up to hit Russia," January 24, 2022: <https://www.reuters.com/business/us-export-rule-that-hammered-huawei-teed-up-hit-russia-2022-01-24/> (accessed February 4, 2022).

2 Julia Pohle and Thorsten Thiel, "Digital sovereignty," *Internet Policy Review* 4/2020: <https://policyreview.info/concepts/digital-sovereignty> (accessed February 4, 2022).

3 Jakob Edler et al., *Technology sovereignty: From demand to concept*, Fraunhofer Institute for Systems and Innovation Research ISI, July 2020: <https://www.isi.fraunhofer.de/content/dam/isi/dokumente/publikationen/technology_sovereignty.pdf> (accessed February 4, 2022).

Contrary to widespread perceptions, conditions in Russia for a thriving digital sector are promising, and prospects for developing technology sovereignty in certain areas are bright. ICT is one of the fastest growing sectors of the Russian economy. Russia is one of the ten countries with the highest number of internet users;[4] making up around 80 percent of its population, they can choose among various internet service providers. While the Russian market also offers highly developed e-commerce and FinTech, Russia's own tech giants provide millions of people in the country with services that range from search engines, social media platforms, and browsers to cab and food delivery services.

The strengthened *siloviki* – those comprising Russia's security apparatus – do undermine Russia's IT prospects as they prioritize control and supervision over economic growth. Yet they are not only driven by security concerns but also by the lucrative promise of digital technologies. In addition, such a promise attracts Russia's economic elite and tycoons close to the Kremlin who have started to stake their claims. Consequently, these actors are wedded together in the digital sector by their overlapping interests, whether they are pecuniary, security-related, or both. Although the regime may profit from such networking in the short term, it will eventually strangle the country's genuine digital development and technological sovereignty.

The preoccupation of Russia's leadership with regime security is increasing; in recent months, it has demonstrated surprisingly skillful control over the technical means of censorship. Yet taking this course is destroying the conditions for a successful and globally competitive IT business. More generally, it will lead to a marginalization of Russia's digital sector. Russia's outlook on foreign policy does not give much reason for optimism either. The current crisis with the West might lead to severe technological sanctions that will hit Russia hard and reveal its heavy dependency on US and European technologies. Russia's prospects as a technological power are therefore becoming more uncertain than ever – despite Moscow's rhetoric on digital sovereignty and regardless of the country's actual capacities and unutilized potential.

This paper analyses the character of Russia's digital sovereignty strategy and the tensions between its main components: *sovereign internet* and *technology sovereignty*. The following section presents the domestic and geopolitical background that has determined Russia's goals in the digital domain. Next, we take a detailed look at the extent to which Russia can control its segment of the internet and be digitally independent from others. In doing so, we differentiate between Russia's achievements and shortages in sovereign internet and technology sovereignty. Accordingly, we focus on control over the internet infrastructure and IT companies, as well as Russia's self-sufficiency in hard- and software and its achievements in innovation policy. The final section contrasts Russia's ambitions for digital sovereignty with realities and assesses the implications of this contrast for the country's domestic and foreign policy.

WHY THE SOVEREIGN INTERNET HAS COME TO TRUMP TECHNOLOGY SOVEREIGNTY

If there is one principle that Russia's leadership seems to take more to heart than any other, it is sovereignty. For years now, "reclaiming sovereignty" has been Vladimir Putin's self-professed political mission. Russia's understanding of a sovereign state is fluid, but, in general, it boils down to the idea of independence from external powers in its domestic and foreign policy. Russia's leaders are especially keen to safeguard their domestic policies from foreign influences ("Westphalian sovereignty") and reestablish control over the cross-border movement of goods, services, capital, people, and ideas ("sovereignty of interdependence").[5] In their view, a sovereign nation needs a strong and effective state, consolidation of society and elites,[6] media free from foreign ownership, and highly developed scientific capability supported primarily by the state.[7]

Russia's understanding of digital sovereignty is tightly embedded in its view of sovereignty in a broader sense, which began to take shape in the early 2000s. In 2005, after being reelected, Putin stressed the following in his annual address to the Federal Assembly (the national legislature): "It is our values that

4 Statista, "Countries with the highest number of internet users as of December 2019," January 31, 2022: <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/> (accessed February 4, 2022).

5 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, 1999).

6 Nikita Garadzha, *Суверенитет* [Sovereignty] (Evropa, 2005).

7 Andrei Kokoshin, *Реальный суверенитет в современной мирополитической системе* [Real Sovereignty in the Modern World Political System] (Evropa, 2006).

determine our desire to see Russia's state independence grow, and its sovereignty strengthened."[8] For the next several years, he would keep repeating this theme about Russia's existential need for sovereignty in his annual addresses[9] until he finally proposed to change the country's constitution in 2020 to protect Russia's "unconditional" sovereignty – and, along with that, to extend his right to stay in power even longer. [10]

An important trigger for Russia's shift to strengthening sovereignty was the conflict with the West that started even before the Crimea annexation in 2014. The "color revolutions" in Georgia in 2003 and Ukraine in 2004, which led to the change of the governmental and political regime in these countries, evoked from Putin robust statements about sovereignty and triggered a broad discussion about so-called sovereign democracy.[11] Fearing a color revolution in Russia, the Kremlin presented the mass demonstrations in both post-Soviet states as being part of the US efforts to export democracy and emphasized the value of Russian sovereignty.

Russia's turn to digital sovereignty is similarly connected to its perception of US predominance in the digital domain and its resulting sense of constrained "Westphalian sovereignty" and "sovereignty of interdependence." The country's quest for digital sovereignty began in 2012 when Putin returned to power as president for the third time, a development that coincided with a crisis of legitimacy for his political regime. With tens of thousands of people demonstrating against fraudulent elections over many months, Putin faced the biggest protests in Russia since the 1990s. The rallies were greatly facilitated by the internet and social media, echoing the earlier Arab Spring. Instead of addressing the people's demand for fair elections and political freedoms, the Kremlin tightened internet regulations and online censorship.

Russia's digital sovereignty strategy was reinforced after Edward Snowden's 2013 revelations about the US surveillance system. In their aftermath, many countries reassessed their dependence on US-based platforms and tried to protect the digital rights of their citizens.[12] For Russian internet users, the outcome was a shift to greater internet control by Russia's secret services.[13] The sanctions introduced by the EU and the United States after the annexation of Crimea and Russia's involvement in the war in Eastern Ukraine from 2014 to 2015 reaffirmed Moscow's perception that its effort to seek digital sovereignty was the right choice. Russia claimed technological independence from Western technologies, charted a course for IT import-substitution, and increased construction of a sovereign internet. These events have significantly shaped the main features of Russia's digital sovereignty path until today: centralized state control over the internet and pushing out foreign social media and tech companies while subjugating the domestic IT sector to the goals of security and regime stability.

As it builds a sovereign internet, Russia finds itself in a rapidly changing world order in which leadership in digital technologies is crucial to great power competition. The world is moving from the globally interconnected internet toward increasing tech nationalism, digital disintegration, and new spheres of influence. Although the conflict between the United States and China is the major rupture line in this trend, other nations – for example, South Korea, Israel, or Taiwan – also play an important role in certain technologies and create dependencies. For Russia, technological partnerships, substitutions, economic sanctions, and, last but not least, its own place in the changing global order have become crucial elements in defining its technology sovereignty.

Russia aspires to go its own way, avoid one-sided dependency, and become the leader of the self-proclaimed "digital non-alignment movement" that unites countries with unlikely chances for digital independence and the wish to escape technological and political dependency on the United

8 Kremlin, Annual Address to the Federal Assembly of the Russian Federation, April 25, 2005: <http://en.kremlin.ru/events/president/transcripts/22931> (accessed February 4, 2022).

9 Kremlin, Presidential Address to the Federal Assembly, December 4, 2014: <http://en.kremlin.ru/events/president/news/47173> (accessed February 4, 2022); Presidential Address to Federal Assembly, February 20, 2019: <http://en.kremlin.ru/events/president/news/59863> (accessed February 4, 2022).

10 Kremlin, Presidential Address to the Federal Assembly, January 15, 2020: <http://en.kremlin.ru/events/president/news/62582> (accessed February 4, 2022).

11 Vladislav Surkov, "Национализация будущего" [The Nationalization of the Future], *Expert*, November 20, 2006: <https://web.archive.org/web/20061205211300/http:/www.expert.ru/printissues/expert/2006/43/nacionalizaciya_buduschego/> (accessed February 4, 2022).

12 Nikhil Kalyanpur and Abraham Newman, "Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened," *Washington Post*, May 25, 2018: <https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/> (accessed February 4, 2022).

13 Miriam Elder, "Russia needs to reclaim its 'digital sovereignty' from US, says MP," *The Guardian*, July 19, 2013: <https://www.theguardian.com/world/2013/jun/19/russia-digital-soveriegnty-nsa-surveillance> (accessed February 4, 2022).

States or China.[14] Hence, to fulfill its ambitions as a great power and have the capacity to act and compete, Russia aims to gain technology sovereignty. It wants to achieve self-sufficiency in hard- and software[15] – starting with developing and primarily using home-grown technologies for state authorities, state owned companies, and critical infrastructure.[16] At the same time, Russia seeks to increase the international competitiveness of its IT and open up new markets, while also offering its leadership as an alternative technological power.[17]

Indeed, Russia has an edge in the technological sphere thanks to human capital – its highly skilled IT specialists and solid academic tradition in engineering and mathematics, a legacy built up over decades in Soviet times. Therefore, it is unsurprising that several leading global companies, including Nginx, Luxoft, JetBrains, Parallels, and Telegram, were founded by Russians. The country's own digital giants, such as Yandex and VK, successfully compete with Big Tech in numerous services and social media networks. Moreover, Russia is especially successful in digital finance; it has become Europe's largest market for digital wallet transactions and shown a very high growth rate in cashless payments.[18] Taken together, these factors put Russia in a good starting position for technological success and competing with the United States, China, and others. But instead, Russia's leadership focuses on internet sovereignty. By equating the notion of "sovereignty" with regime security and making this a top priority, the Kremlin limits the country's technological success and damages its technological sovereignty in real terms.

PUTIN HAS ABANDONED DIVERSIFICATION

For years, Russia's leadership has been trying to diversify the country's economy and find alternative drivers of advancement. In 2009, a strong push for innovation was set by then President Dmitry Medvedev. In his article "Go Russia!", Medvedev formulated his vision for Russia's future development, in which the country's well-being is ensured by a "smart" economy, technology exports, and innovative products rather than by raw materials.[19] The development of home-grown technologies and IT, as well as the replication of the Silicon Valley's success in Russia, were a significant part of his economic vision and political project.

In 2012, shortly before he retook the presidency, Vladimir Putin also publicly recognized the need for a "new economy working on a modern technological basis."[20] He called for diversifying the economy away from the resource-led model and instead developing innovations and regaining technological leadership. Such a course, however, would require genuine economic reform and the strengthening of property rights and the rule of law. This, in turn, would lead to emerging independent economic actors, potentially threatening the regime. Facing mass protests after the elections in 2011 and 2012, Putin did not take that risk. He abandoned Medvedev's plans and mostly preserved the existing economic model. Putin perfectly understands that a broad diversification of the economy and robust economic growth would also instantly lead to a diversification of wealth and power with uncontrollable actors, new networks, and an even more empowered middle class than he already saw on Moscow's streets during the protests. Instead of diversification, Putin took the course to sovereignty – strengthening state control over the economy and politics – and closing off his ruling circle.

14 Andrei Bezrukov, Mikhail Mamonov et al., *Realpolitik в «цифре»: суверенитет, союзы и неприсоединение XXI века* [Realpolitik in the digital sphere: sovereignty, alliances, and non-alignment in the 21st century], Report of the Valdai International Discussion Club, September 2021: <https://ru.valdaiclub.com/files/39047/> (accessed February 4, 2022).

15 Unified Register of Russian Programs for Computers and Databases: <https://reestr.digital.gov.ru> (accessed February 4, 2022).

16 Kremlin, Strategy for Information Society Development until 2030 approved, May 10, 2017: <http://en.kremlin.ru/acts/news/54477> (accessed February 4, 2022).

17 The National Technological Initiative (NTI): <https://nti2035.ru/nti/> (accessed February 4, 2022).

18 RBC, "BCG сообщила о «русском чуде» в сфере карточных платежей" [BCG reported on the "Russian miracle" in card payments], October 3, 2019: <https://www.rbc.ru/finances/03/10/2019/5d94d4459a79473994997fe0> (accessed February 4, 2022).

19 Kremlin, "Dmitry Medvedev's Article, Go Russia!", September 9, 2009: <http://en.kremlin.ru/events/president/news/5413> (accessed February 4, 2022).

20 Vladimir Putin, "«Нам нужна новая экономика»" [We need a new economy], *Vedomosti*, January 30, 2012: <https://www.vedomosti.ru/politics/articles/2012/01/30/o_nashih_ekonomicheskih_zadachah> (accessed February 4, 2022).

Russia's Goals for Its Sovereign Internet

The political regime created under Vladimir Putin is nearing another major legitimation crisis. Due to weak economic performance and the lack of political reforms, it is becoming more and more difficult to legitimize the irrevocability of power for so many years. In the early 2000s, Russia's economy grew rapidly due to very high oil prices, super-charging ordinary people's real incomes. Russia's success and well-being were associated with Putin and led to high popularity despite his lack of structural reforms and weak rule of law. But these boom years are long over. The Russian economy has been growing at about 1 percent per year for more than a decade now. The real income of Russians has declined for the eighth year in a row, despite official reports on the constant increase in wages.[21]

Just as the rise in real income was once directly associated with Putin, Russia's stagnation and decline are now associated with him today. Even if Putin's approval ratings remain relatively high at around 65 to 69 percent,[22] support for his presidential activities[23] and the main state institutions, including the ruling party, is constantly declining.[24] Consequently, as the regime's legitimation becomes more problematic, it seeks to play a greater role in determining the means and use of the internet in Russia.

A free internet facilitates exactly what the centralized Russian regime fears the most: uncontrollable means of disseminating information, non-hierarchical debates, and independent channels for collective action. That is why internet policy is geared decisively toward "content security," limiting any information that the regime perceives as politically subversive. Even if the state continues to rely on selective law enforcement in its fight against critics in the online sphere,[25] foreign players on the IT market pose a threat since they are hard to monitor and control. Therefore, a Russian sovereign internet should curtail opposition activity on social media and keep social discontent and protests at bay. Russia's authorities aim to expand their tools of technological censorship and force foreign social media companies to cooperate – or push them out of the Russian market. At the same time, they seek to gain direct control over domestic tech companies and channel citizens onto Russian social media and services.

(MIS-)MATCHING THE GOALS: RUSSIA'S SUCCESSES AND SHORTFALLS

A closer look beyond the statements and proclaimed goals of Russia's leadership reveals sober realities. The Russian state is actively building up its sovereign internet and gaining more and more direct control over society and the domestic IT market. At the same time, Russia remains highly dependent on others and has failed to utilize its technological potential for the country's digitally sovereign future. In this chapter, we map and analyze the implementation of both the sovereign internet and technology sovereignty to provide a detailed picture.

Sovereign Internet: Succeeding in Censorship and Securing the Regime

Over the last several years, content security and a sovereign internet have been actively implemented. A mere decade ago, Russians made use of the unfettered internet to keep themselves informed or organize protests. Today, state authorities use digital technology to hinder free communication, prevent the dissemination of critical information, and control both society and internet companies.

Controlling the Internet Infrastructure: From Blacklist to Black Box

Since 2012, when Putin returned to the presidency amid widespread protests, Russia has introduced extensive legislation to control the internet and restrict free access to information. Initially, this control was indirect and took the form of a so-called blacklist of prohibited websites in Russia. The Russian authority Roskomnadzor monitored and updated this list and ordered host providers to remove URLs with undesired information. If the host did not comply, Roskom-

21 Finmarket, Реальные доходы россиян снижаются восьмой год подряд [Real income of Russians declined for the eighth year in a row], February 5, 2021: <http://www.finmarket.ru/main/article/5406082> (accessed February 4, 2022).

22 Levada Center, Одобрение деятельности Владимира Путина [Approval of Vladimir Putin's work]: <https://www.levada.ru/indikatory/> (accessed February 4, 2022).

23 Levada Center, Президентские рейтинги и положение дел в стране [Presidential ratings and the state of affairs in the country]: <https://www.levada.ru/2021/02/04/prezidentskie-rejtingi-i-polozhenie-del-v-strane/> (accessed February 4, 2022).

24 Denis Volkov, "Демобилизация и поляризация: парламентские выборы в зеркале опросов общественного мнения" [Demobilization and polarization: Parliamentary elections in the mirror of public opinion polls], Liberal Mission Foundation, November 18, 2021: <https://liberal.ru/lm-ekspertiza/demobilizacziya-i-polyarizacziya-parlamentskie-vybory-v-zerkale-oprosov-obshhestvennogo-mneniya> (accessed February 4, 2022).

25 Milan Czerny, "Selective Law Enforcement on the Runet as a Tool of Strategic Communications," *Defense Strategic Communications*, February 1, 2021: <https://stratcomcoe.org/publications/selective-law-enforcement-on-the-runet-as-a-tool-of-strategic-communications/11> (accessed February 15, 2022).

nadzor turned to the Internet Service Providers (ISPs) and required them to block access to those sites.[26]

This system proved to be ineffective. Hence, the state moved to a system of more direct technical control of the internet. The major shift came in 2019 after the enactment of the so-called Sovereign Internet Law.[27] In short, this law stipulates that ISPs must install Deep Packet Inspection (DPI) – so-called black boxes, which are installed at the hubs of internet providers to analyze both data packets and the content of communications. They allow requests of internet users to certain websites to be monitored, filtered, and throttled, and certain content to be blocked. Since then, the efficiency of Roskomnadzor's task has significantly increased: now it can independently limit the speed of access to certain websites and block targeted information without risking major disruption across the RuNet, the internet within Russia.

As of today, it is likely that all large providers comply with the law and have installed the DPI systems more or less across the country.[28] There is solid evidence suggesting that the DPI systems work and their efficacy has made them a go-to instrument for Russian censorship. Because Twitter refused to block posts, Roskomnadzor slowed down that social network in Russia in March 2021. Despite some collateral damage,[29] the Twitter throttling was effective enough – also because it made clear that the authorities were now much better equipped to censor critical voices. For an ordinary user who has no specific IT skills, bypassing the bans is hard. Despite the rather decentralized structure of the internet in Russia, this and several other cases prove that the state has somewhat succeeded in building up a censorship apparatus.[30]

Shortly before the September 2021 Duma election, Roskomnadzor again demonstrated the strength of its censorship capability. It not only went after certain websites of the opposition, but it also aimed to shut down bypass tools such as those designed to duplicate the blocked sites and keep them accessible. The result: without broader collateral damage to the internet, it blocked almost every platform associated with the opposition leader Alexei Navalny as well as his mirror website. In the same month, Roskomnadzor blocked access to six providers of Virtual Private Networks (VPNs) that were allowing access to prohibited content in Russia.[31] Just three months later, it started to successfully block the digital anonymity service Tor by again utilizing DPI.[32] In Russia, which has the second largest user base of Tor after the United States, people are actively using it to circumvent authorities' restrictions.

In the near future, Google services such as YouTube, which is a very popular social media platform in Russia, could also be affected by throttling via DPI. Here, however, major collateral damage is to be expected. YouTube uses the Google Global Cache, one of the world's largest Content Delivery Networks (CDNs).[33] If Russian authorities block one of these websites, they could end up blocking many more. It is questionable whether Roskomnadzor wants to take this risk. Furthermore, a slowdown of YouTube or other widely used social media platforms such as WhatsApp or Instagram, which are much more popular than Twitter in Russia, would affect many more people, potentially leading to greater resentment among the population. To circumvent this problem, authorities are trying to nudge users onto Russian social media networks that they can better surveil – albeit with no significant impact on the numbers of users for the US firms so far (see figure 1).

Russian Domain Name System: Protecting RuNet from Being Cut-Off and Increasing Content Security

Under the Sovereign Internet Law, Russia also plans to build its own Domain Name System (DNS) and infrastructure managed by Roskomnadzor as an alter-

26 Andrei Soldatov, "Security First, Technology Second," DGAP Policy Brief, March 7, 2019: <https://dgap.org/en/research/publications/security-first-technology-second> (accessed February 4, 2022).

27 Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law,'" DGAP Analysis, January 16, 2020: <https://dgap.org/de/node/33332> (accessed February 4, 2022).

28 *Kommersant*, "Провайдеров Накачали «суверенным Интернетом»" [Providers were pumped full of "sovereign Internet"], September 18, 2020: <https://www.kommersant.ru/doc/4494156> (accessed February 4, 2022).

29 Jim Salter, "A Russian ISP Confirms Roskomnadzor's Twitter-Blocking Blooper," *Ars Technica*, March 11, 2021: <https://arstechnica.com/gadgets/2021/03/a-russian-isp-confirms-roskomnadzors-twitter-blocking-blooper/> (accessed November 29, 2021).

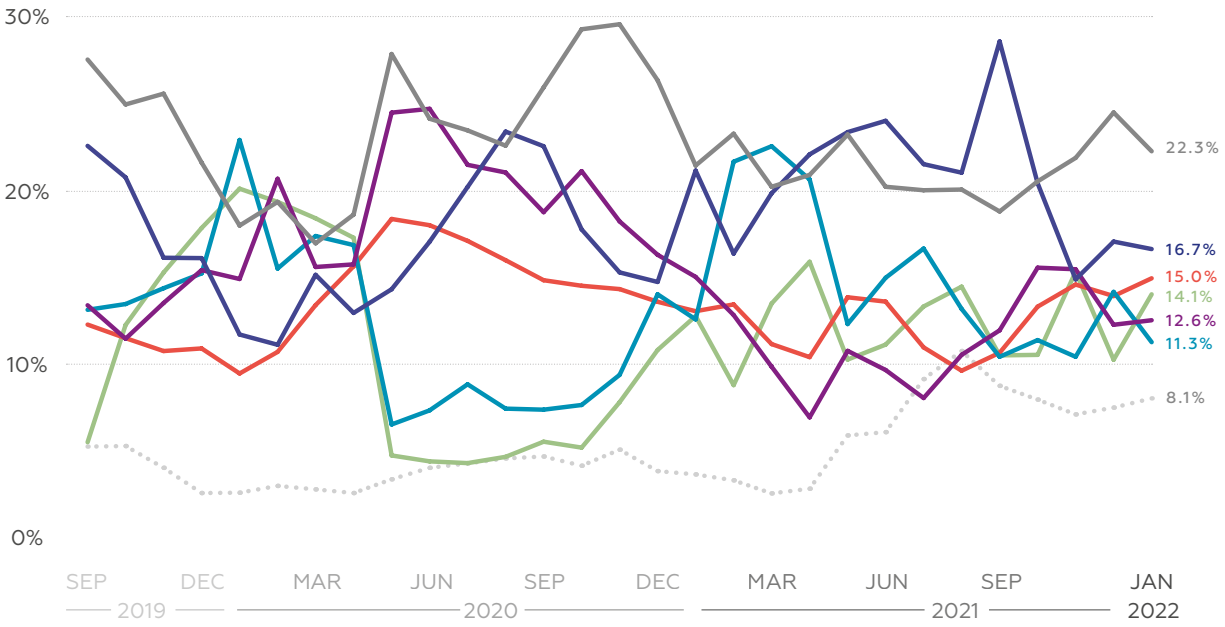
30 Reethika Ramesh, Leonid Evdokimov, and Roya Ensafi, "Censorship in Russia," *Censored Planet*, November 6, 2019: <https://censoredplanet.org/russia> (accessed November 29, 2021).

31 *The Moscow Times*, "Russia Blocks VPN Providers in Ongoing Internet Crackdown," September 3, 2021: <https://www.themoscowtimes.com/2021/09/03/russia-blocks-vpn-providers-in-ongoing-internet-crackdown-a74966> (accessed February 4, 2022).

32 Chris Stokel-Walker, "Russia's Internet Censorship Machine Is Going After Tor," *Wired*, December 10, 2021: <https://www.wired.com/story/russia-block-tor-censorship/?mbid=social_twitter&utm_brand=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter> (accessed February 4, 2022).

33 A CDN is a network of geographically distributed servers that caches websites in order to make them available to the user more quickly.

1 – SOCIAL MEDIA STATS OF THE RUSSIAN FEDERATION ACCORDING TO THEIR TRAFFIC GENERATION CAPABILITIES, SEPT 2019 – JAN 2022



Source: StatCounter Global Stats. Accessed February 4, 2022

native to the one currently globally managed by the International Corporation for Assigned Names and Numbers (ICANN). In a nutshell, the DNS can be considered the backbone of the internet, serving as its "phone book" by allocating domain names and associating them with IP addresses.

There is no doubt that this step represents a tall technical challenge; no single country has yet created a system that could work in parallel to the worldwide DNS. But the Kremlin has its reasons. It sees ICANN as being dominated by the United States and fears that Russia could get cut off from the global internet from outside – even if this is technically almost impossible.[34] Since the Kremlin started criticizing ICANN in 2012, Russia has pursued more independence from it and pushed for state control over the national DNS. This is crucial for Russia not only in the context of internet governance in general, but also for achieving greater control over information and maintaining the regime's stability.

The problem for Russia's censors comes in the form of modern internet protocols that make the monitoring and filtering of undesirable information for the DPI system extremely difficult. Such protocols do not allow the Russian authorities to see which site the user is accessing.

Many large DNS providers, such as US-based Google and Cloudflare as well as the Russian internet giant Yandex, are successfully switching to these new protocols. Google is also adapting its Chrome browser – the most popular one in Russia – accordingly. The problem for Russia's regulator is that these new protocols render DPI technology almost useless. Consequently, Russia's government suggested a law to ban them.[35] According to the proposal,

34 Epifanova, "Deciphering Russia's 'Sovereign Internet Law'" (see note 27).

35 Maria Kolomychenko, "Russia's Digital Development Ministry wants to ban the latest encryption technologies from the RuNet," *Meduza*, September 21, 2020: <https://meduza.io/en/feature/2020/09/22/russia-s-digital-development-ministry-wants-to-ban-the-latest-encryption-technologies-from-the-runet> (accessed January 28, 2022).

any website that uses internet protocols that hide "the name of a web page" will be banned inside Russia within one working day.

Furthermore, in September 2021, Russia's major state-backed telecom provider, Rostelecom, offered to replace DNS servers nationwide with Russia's national DNS.[36] This was followed by several tests that resulted in Roskomnadzor successfully blocking the encrypted DNS protocols of Google and Cloudflare for a time. This process, however, has many problematic aspects. First, the encrypted protocols are extremely secure and therefore make it difficult for criminals to intercept them via Man in the Middle (MITM) attacks. If they are banned, criminals can operate more easily. Second, access to sites can be precisely controlled via a state DNS, opening the door to censorship. Third, a blanket block of the DNS services of Cloudflare and Google would probably lead to massive disruptions and failures because many DNS requests from users will not be able to be resolved, resulting in people simply not being able to get to a website to see information. As already mentioned, some browsers already use DoH. Operating systems such as Android – the second most used OS in Russia – communicate with Google's DNS servers by default. Thus, it follows that switching to a national DNS would mean that both browsers and operating systems would need to be reconfigured, which could cause massive disruptions for thousands of companies and millions of average users in Russia.[37]

Such possible disruption of the internet in Russia, however, does not seem likely to deter the authorities from implementing the national DNS. Since early 2021, Russian internet service providers are required to connect to the new national DNS – although they can still connect to the worldwide DNS in parallel. Some companies that have not established a connection to the national DNS have already been fined.[38] However, as the fines for companies are currently low, some companies prefer to pay them and not connect to the national DNS to not be disrupted by incidents that such a connection could cause. These disruptions could cost them more than the fines.[39] This example, in turn, shows that Russian authorities still have technical limits in censoring information because of technical dependency on international internet companies. Therefore, the state has gradually deployed pressure and threatened IT companies with fines and prosecution in an attempt to subjugate them.

THE EFFECT OF MODERN DNS PROTOCOLS

Classic DNS requests are made via plaintext. The resulting connection is encrypted via the secure HTTPS protocol and hidden from the eyes of authorities. This means, for example, that authorities can see which website a user is accessing (e.g., YouTube.com), but cannot see which video that user is watching. Modern encrypted protocols such as DoH (DNS over HTTPS) and DoT (DNS over TLS) can even make the request encrypted, meaning that authorities can therefore not even see which site the user is accessing.

Subjugating RuNet:
Pushing Foreign IT Out of the Russian Market and Taking Over Domestic Tech

US-based companies are the primary targets for accusations of what Moscow calls interference in Russia's domestic politics. The state authorities have sued and fined Google, Facebook, and Twitter several times for failing to remove illegal or banned content. This usually ranges from posts related to suicide, child pornography, and drugs to messages calling for Russians to protest. In practice, such fines have become a censorship mechanism and a pressure tool against social media[40] – although, ranging from $10 thousand to $100 thousand, they had been rather token for such IT giants. This situation escalated on Christmas Eve 2021, however, when Russia fined Google $98.4 million

36 BFM.RU, "«Ростелеком» Собирается Заменить На Собственные Аналоги Публичные DNS-Серверы Google и Cloudflare" [Rostelecom is going to replace Google and Cloudflare Public DNS Servers with its own analogues], September 14, 2021: <https://www.bfm.ru/news/481358> (accessed January 28, 2022).

37 Valeri Romanov and Doni Jabborov, "«Все отвалится»: как запрет серверов Google сломает рунет" ["Everything will fall off": how banning Google servers will break RuNet], *Газета.ru*, September 14, 2021: <https://www.gazeta.ru/tech/2021/09/14/13983698/googlednsblock.shtml> (accessed November 30, 2021).

38 Anastasia Gavrilyuk, "Доменирующее положение" [Domain's position], *Kommersant*, August 31, 2021: <https://www.kommersant.ru/doc/4966108> (accessed November 30, 2021).

39 Ibid.

40 For example, shortly after the countrywide protest in support of opposition leader Alexei Navalny, Russia filed a lawsuit against five social media platforms for not deleting posts urging children to take part in illegal protests. See: Reuters, "Russia sues Google, Facebook, Twitter for not deleting protest content – Ifax," March 9, 2021: <https://www.reuters.com/article/us-russia-politics-social-media-fines-idUSKBN2B1130> (accessed January 28, 2022).

and Facebook/Meta $27 million for failing to remove banned content.[41] The signal was clear: foreign companies cannot continue their business in Russia without major losses if they do not cooperate with the authorities in censoring RuNet.

In 2021, another unprecedented example showed that pressure can be effective in forcing foreign companies to cooperate. On the first day of the Duma elections in September, Google and Apple removed an app created by Alexei Navalny's team for tactical voting[42] from their stores in Russia.[43] Google also blocked access to the Google Docs and YouTube videos posted by Navalny's team that contained the list of candidates for this tactical voting. Russian authorities had threatened the companies with criminal prosecution of their employees if they did not comply with the demand to block the app. Also, the popular messenger app Telegram cooperated with the state in a similar way, blocking bots that supported the tactical voting.

To have greater control over foreign tech companies, a new law was adopted in summer 2021.[44] It requires foreign platforms with a daily user base of over 500,000 to open representative offices in Russia. Additionally, they must add a feedback form for Russian users on their website, register a personal account on Roskomnadzor's website for interaction with the authorities, and limit access to information that "violates Russian law" – meaning censor undesired information.

According to Roskomnadzor's register, 13 foreign companies owning 22 information services and resources need to comply with the new law.[45] Among these companies are Google, Meta (formerly Facebook),[46] Apple, Twitter, TikTok, and Telegram. The law came into force on January 1, 2022, and gave the authorities various "enforcement measures" in case of noncompliance that include restricting money transfers and payments, slowing down local traffic, and completely blocking access to the online resource. The extent to which Roskomnadzor will apply these measures remains to be seen, but the authorities certainly now have additional tools designed to force foreign IT companies to cooperate and deprive Russian users of free access to information. Apple, Twitter, and other companies have already started to comply with the new law and registered a personal account on Roskomnadzor's website.[47]

While pressure has been put on foreign companies, there has also been a significant shift toward greater control of domestic tech giants. In December 2021, "Russia's Facebook" – the country's largest homegrown social media platform VKontakte (VK) – was taken over by companies tied to state-run gas giant Gazprom and Yuri Kovalchuk, one of Vladimir Putin's closest allies. Almost immediately after the deal, Vladimir Kiriyenko, a son of President Putin's first deputy chief of staff, was appointed as VK's new CEO. The takeover establishes a precedent for the state's move from a "control through ownership" model,[48] i.e., encouraging Kremlin-adjacent oligarchs to take over the digital sector, to direct control over Russian tech companies. For the first time in the history of the RuNet, one of the most popular social media platforms in the country and a powerful domestic IT player will be controlled completely by the state.[49] The deal is also a prominent example of the redistribution of the lucrative digital market among the trusted allies of Russia's leadership whose pecuniary and security-related interests overlap. By granting control over a big business, the leadership hopes to keep its political-economic network together, ensure content security, and sustain political stability.

41 *The Moscow Times*, "Russia Fines Google, Meta Record $125M for Banned Content," December 24, 2021: <https://www.themoscowtimes.com/2021/12/24/russia-fines-google-100m-for-banned-content-a75924> (accessed January 28, 2022).

42 A tactical voting concept called "Smart Voting" features a list of candidates that Navalny's team sees as best placed to defeat their competitors from the ruling United Russia party; the team suggested these candidates to voters shortly before election day.

43 Max Seddon and Madhumita Murgia, "Apple and Google drop Navalny app after Kremlin piles on pressure," *Financial Times*, September 17, 2021: <https://www.ft.com/content/faaada81-73d6-428c-8d74-88d273adbad3> (accessed January 28, 2022).

44 Official Internet Portal of Legal Information, Federal law No. 236-FZ "О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации" [On the activities of foreign persons in the information and telecommunications network "Internet" on the territory of the Russian Federation], July 1, 2021: <http://publication.pravo.gov.ru/Document/View/0001202107010014?index=0&rangeSize=1> (accessed January 28, 2022).

45 Roskomnadzor, List of foreign persons operating in the Internet on the territory of the Russian Federation, November 22, 2021: <https://236-fz.rkn.gov.ru/agents/list> (accessed January 28, 2022).

46 The parent organization of Facebook, Instagram, and WhatsApp.

47 *Kommersant*, "Twitter начал исполнять российский закон о «приземлении»" [Twitter started enforcing Russia's "landing" law], January 25, 2022: <https://www.kommersant.ru/doc/5182021> (accessed January 28, 2022).

48 Carolina Vendil Pallin, "Internet control through ownership: the case of Russia," *Post-Soviet Affairs* Volume 33, 2017 – Issue 1, pp. 16–33: <https://www.tandfonline.com/doi/abs/10.1080/1060586X.2015.1121712?journalCode=rpsa20> (accessed January 28, 2022).

49 Petr Mironenko and Irina Malkova, "Why Alisher Usmanov sold VK to Sogaz," *The Bell*, December 5, 2021: <https://thebell.io/pochemu-alisher-usmanov-prodal-vk> (accessed January 28, 2022).

In the case of another Russian tech giant – Yandex, which is registered in the Netherlands – the state has indirect control over the strategic decisions of the company. Yandex was forced to build state control into its corporate governance structure and adapt to the legislation limiting foreign ownership of major internet companies.[50]

As it gains more control over Russian IT companies, the state is nudging users toward primarily domestic services. As of April 1, 2021,[51] all smartphones sold in Russia have been required to have Russian applications from a government-approved list preinstalled – among them, a social media platform, search engine, email service, payment system, and maps. The products of companies such as Yandex; VK; MyOffice, the Russian analogue of Microsoft Office; Kaspersky, a provider of cybersecurity services; and others will benefit from this protectionist measure. In addition, desktops and laptops sold in Russia must be equipped with the Yandex browser, the MyOffice suite, and the Kaspersky antivirus program as their standard software.[52]

Manufacturers that do not comply will get fined. Interestingly, although the bill was initially labeled by the media as the "anti-Apple law" – referring to the US manufacturer that does not preinstall any software on its devices other than its own – Apple has complied. The company turned out to have enough room for maneuver with the Russian state to make a compromise. Since iOS 14.3, Russian apps are suggested to the user when setting up an iPhone, which can then be installed with one click.

The strategy behind this approach is clear: Russian users should primarily use Russian internet services, which the state can easily surveil and manage. Since international companies such as Google and Facebook cannot be banned immediately, they will simply be so severely disadvantaged that users will leave them and instead move – apparently voluntarily – to a network in which the state can exercise greater social control.

Technology Sovereignty: Staying Dependent and Missing the Chance for Tech Power

Compared to its progress on the sovereign internet, Russia has achieved less significant results in technology sovereignty. This confirms the assessment that the state has prioritized content security and regime stability over economic growth and technological leadership.

To guarantee that its long-term goal of self-sufficiency in IT can be met, Russia would need to create equivalents for the entire foreign tech stack – hardware, software, and data. This huge challenge is almost impossible to achieve in the short and medium term. Despite its proclaimed course, Russia is still dependent on crucial foreign technologies and global supply chains. Forced IT import substitution, which privileges a closed group of companies and creates artificial IT markets for them, would lead to the marginalization of its IT sector and digital economy.

Since we have limited space in this paper, we will only focus our analysis on a few industries that we assume will play the most important role in the realm of technology sovereignty for Russia. When it comes to Russia's progress on achieving self-sufficiency in the hardware sector, we will look at central processing units (CPUs) and the creation of domestic 5G solutions. In the software sector, we will turn to operating systems, software and repository hosting platforms, and cloud computing solutions. We will then close this section by assessing the effects of Russia's digital and innovation policy on its pursuit of technology sovereignty, including in the area of artificial intelligence (AI).

Self-Sufficiency in the Hardware Sector

Especially in the hardware sector, Russia's current position is weak. Although the country has a few of its own manufacturers of processors, proper self-sufficiency will hardly be possible anytime soon.

Central Processing Units (CPUs)

In Russia, processors are mainly developed by two companies, both of which have already successfully

50 Max Seddon, "Yandex agrees restructuring with Kremlin," *Financial Times*, November 18, 2019: <https://www.ft.com/content/999e3ca6-09db-11ea-bb52-34c8d9dc6d84> (accessed January 28, 2022).

51 Official Internet Portal of Legal Information, Federal law No. 425-FZ "О внесении изменения в статью 4 Закона Российской Федерации «О защите прав потребителей»" [On Amendments to Article 4 of the Law of the Russian Federation "On Protection of Consumer Rights"], December 2, 2019: <http://publication.pravo.gov.ru/Document/View/0001201912020057> (accessed December 9, 2021).

52 Official Internet Portal of Legal Information, "Распоряжение Правительства Российской Федерации" [Decree of the Government of the Russian Federation No. 2607-r dated September 18, 2021], September 27, 2021: <http://publication.pravo.gov.ru/Document/View/0001202109270018?index=0&rangeSize=1> (accessed December 9, 2021).

launched microchips for use in computers: Baikal Electronics and the Moscow Centre of SPARC Technologies (MCST).

Baikal Electronics, a subsidiary of the Russian supercomputer company T-Platforms, manufactures CPUs based on the ARM architecture. ARM is a British semiconductor company owned by SoftBank Group, a multinational conglomerate holding company based in Japan. To use the architecture, Baikal Electronics pays fees to ARM. This means that it is not independent of Western companies and cannot only rely on Russian solutions.

From a technical point of view, the choice of ARM is obvious: it is the leading chip design company in the world and has been praised for being a very powerful and highly energy-efficient platform. Originally, ARM architecture was mainly used in mobile phones, but, more and more, it is finding its way into other devices such as laptops. For example, with its M1 chip, Apple has started to produce its own CPUs based on ARM, breaking benchmark records in terms of performance and power-management.

ARM chips of the BE-M1000 type for Baikal are produced by the Taiwanese company TSMC, one of the world's leading semiconductor manufacturers.[53] In fall 2021, Baikal received the first batch of its ARM chips; however, the number of delivered units per month – 5,000 – is very low. In the long term, the company plans to obtain up to 15,000 units per month from TSMC.[54]

The Baikal processors are supposed to be used in the computers of state-owned companies. According to outside assessments, the processor is comparably slow: it has roughly the same performance as low-end Intel CPUs from 2017 that were designed to handle only light office tasks.[55]

Apart from Baikal's CPU and its modified operating system Astra Linux, none of its other components are designed or manufactured in Russia. Given that the country currently has no production capacities for memory chips and storage drives, it is therefore fully dependent on foreign manufacturers.

HOW A CPU ARCHITECTURE WORKS

In very simplified terms, a computer's CPU architecture links its hardware to its software and defines what a CPU needs to do. CPUs work when given specific instructions – a so-called instruction set – that tells the processor how to move data and perform calculations. Different CPUs use different instruction sets, each of which has their own respective advantage, for example creating more performance while consuming less power.

The second Russian computer manufacturer, MCST, uses its own Elbrus architecture, which works with the VLIW method. While VLIW (Very Long Instruction Word) has proven itself in a very specific application area, it is not suitable for the mass market. The complicated programming paths within the processor make it too energy intensive for operations in everyday applications and consumer devices.[56]

Elbrus computers are designed according to Russia's governmental requirements for security and reliability and only used by customers whose work is designated as sensitive to the state, such as the Ministry of the Interior and some oil and gas companies.[57] Elbrus plans on releasing its newest CPU soon, the so-called 16C, which will have more cores and run considerably faster than its older versions. In comparison to today's leading-edge processors though, Elbrus will still be significantly slower.[58] Elbrus also depends on chips manufactured by TSMC in Taiwan.

The state corporation Rostec – together with the developer Yadro, a subsidiary of ICS Holding that belongs to Alisher Usmanov, a Russian oligarch close to the Kremlin – has now set its sights on produc-

53 Statista, Leading semiconductor companies (including foundries) from 2019 to 2021, by sales revenue, December 2021: <https://www.statista.com/statistics/283359/top-20-semiconductor-companies/> (accessed February 4, 2022).

54 Anton Shilov, "Russia Gets First Batch of Arm-Based Homegrown SoCs: All 66 Kgs of Them," *Tom's Hardware*, October 15, 2021: <https://www.tomshardware.com/uk/news/first-baikal-socs-delivered-to-russia> (accessed February 4, 2022).

55 Jason R. Wilson, "Second-Generation Baikal Electronics BE-M1000 CPUs Begins Shipping From Chip Fab Giant TSMC," *Wccftech*, October 19, 2021: <https://wccftech.com/second-generation-baikal-electronics-be-m1000-cpus-begins-shipping-from-chip-fab-giant-tsmc/> (accessed February 4, 2022).

56 VLIW: Difficulties of Implementation: <http://www.ecs.umass.edu/ece/koren/architecture/VLIW/1/difficulties.html> (accessed November 27, 2021).

57 TAdviser, Elbrus-16C: <https://tadviser.com/index.php/Product:Elbrus-16C> (accessed November 27, 2021).

58 Anton Shilov, "Russian Company Tapes Out 16-Core Elbrus CPU: 2.0 GHz, 16 TB of RAM in 4-Way System," *Tom's Hardware*, October 7, 2020: <https://www.tomshardware.com/uk/news/russian-company-tapes-out-16-core-elbrus-cpu-20-ghz-16-tb-of-ram-in-4-way-system> (accessed November 27, 2021).

ing another Russian processor.[59] Rostec aims to create a new processor for use in computers at schools, universities, and hospitals by 2025. It is not yet possible to say how powerful this new CPU will be; although the architecture (RISC-V), the number of cores (8), the projected clock speed (2 GHz), and the production size (12 nm) are known, no clear conclusions can be drawn about performance. Such assessment is difficult mainly because the Instruction Set Architecture (ISA) of RISC-V, which creates the link between hardware and software and defines what a processor is capable of, is not yet used as a standard. For conventional ISAs, processor manufacturers must pay royalties to companies like ARM or Intel. RISC-V, however, is open source and therefore available for free. Its new and largely unproven architecture does not yet make it possible to say whether the project will be successful at all – let alone in the tight timeframe foreseen by Rostec. Yet even if the project were to be completed by 2025, it is unlikely that the processor will be able to compete with the likes of Intel or AMD, major manufacturers of computer processors both based in the United States, in terms of performance. Admittedly, the Russian state's main objective is not to be best in performance but to reduce its dependence on Western systems by providing workable alternatives.[60]

Despite the developments at Baikal Electronics and MCST, Russia is not able to produce its own chips. Initially, the Elbrus CPU was supposed to be produced by Russia's biggest manufacturer of microelectronics, the Mikron Group. This project never materialized.[61] In fact, Russian manufacturers do not seem to be able to produce any chips with small Dennard scaling (see box). Both the Elbrus and the Baikal CPUs are manufactured by TSMC in Taiwan – on machines that TSMC needs to order in Europe. Moreover, as already mentioned, Russia does not have the capability to manufacture memory chips and storage drives. Thus, there is no independent, purely Russian supply chain.

PRODUCING ADVANCED CPUs

Photolithography machines are needed to produce CPUs. The most advanced producer of these machines – and the only one using the Extreme Ultraviolet Lithography (EUVL) required to manufacture modern chips with smaller Dennard scaling, i.e., in very simplified terms those having smaller transistors that make CPUs more powerful – is a Dutch company called ASML. It effectively holds a monopoly in this domain.[62]

Russia can produce other types of chips for civil and military use. The Mikron Group, for example, sells products including bank card microcontrollers, power management chips, and radio frequency identification (RFID) chips.[63] Russian companies such as Angstrem used to produce chips for military use but are now bankrupt.[64] Evidence suggests, however, that Russia almost exclusively imports chips for highly sophisticated applications.[65]

5G

It is also complicated for Russia to develop domestic solutions for the hardware required for its fifth-generation cellular network, so-called 5G.

Russia's plans to use only domestic systems and software in building up its 5G network have created a lot of uncertainty for domestic mobile operators. Currently, the country has none of its own equipment and therefore relies on foreign vendors with whom Russian operators have cooperated for several decades to establish the previous generations of the country's cellular network.[66] But this policy plays into the hands of the state corporation Rostec, one of the

59 Tatyana Isakova: "«Ростех» разработает процессоры для школ, вузов и больниц" [Rostec will develop processors for schools, universities, and hospitals], *Vedomosti*, July 14, 2021: <https://www.vedomosti.ru/technology/articles/2021/07/14/878092-rosteh-razrabotaet-protsessori> (accessed October 4, 2021).

60 Robin Mitchell, "Russia Producing Its Own Motherboards, and the Brilliance of VLIWs," *Electropages*, May 25, 2021: <https://www.electropages.com/blog/2021/05/russia-producing-its-own-motherboards-and-brilliance-vliws> (accessed October 4, 2021).

61 TAdviser, Elbrus-16C (see note 57).

62 *The Economist*, "How ASML became chipmaking's biggest monopoly," February 29, 2020: <https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly> (accessed February 15, 2022).

63 Mikron, RFID Products: <https://en.mikron.ru/products/rfid-chip-inlays-maps/> (accessed February 4, 2022).

64 Svetlana Yastrebova and Ivan Safronov, "ВЭБ хочет передать оборудование «Ангстрем-Т» государству" [VEB wants to transfer Angstrem-T equipment to the state], *Vedomosti*, January 16, 2020: <https://www.vedomosti.ru/economics/articles/2020/01/16/820791-veb-peredat> (accessed February 4, 2022).

65 Michael Peck, "Russia's Military Admits It Needs Western Technology," *The National Interest*, August 3, 2019: <https://nationalinterest.org/blog/buzz/russia's-military-admits-it-needs-western-technology-70916> (accessed February 4, 2022).

66 Leonid Kovachich, "Who Will Get a Slice of Russia's 5G Pie?", Carnegie Moscow Center, December 27, 2021: <https://carnegiemoscow.org/commentary/86092> (accessed February 4, 2022).

main drivers of import substitutions.[67] After it lobbied for the exclusive use of Russian-made equipment, it received a major contract to manufacture 5G technology and billions of rubles in state subsidies.[68] However, Rostec's equipment will not be ready until 2024 at the earliest – a long time in a rapidly changing technology market. Moreover, given that Russian companies have no expertise in mass-producing 5G equipment and there are no Russian 5G patents in international ratings, the timespan for building 5G equipment from the ground up by 2024 is very ambitious, if not unrealistic.

A way to build up 5G and claim it as Russian might be the localization of foreign technology production on Russian territory. This could also provide a certain level of control over the 5G infrastructure. In fall 2021, the Finnish corporation Nokia and Yadro, a Russian manufacturer of computing equipment, agreed to create a joint venture for the production of base stations of 4G and 5G standards in Russia. Production will be done at the Yadro plant under construction in Dubna, a city close to Moscow.[69] In addition, Nokia software licenses will be transferred and a research and development (R&D) center for the advancement of 4G and 5G technology will be established. Other foreign vendors, such as China's Huawei and ZTE, as well as Sweden's Ericsson, have also expressed interest in localization.

For now, it seems like Russia is trying to avoid one-sided dependency and find balance among the leading companies in this field – Nokia, Ericsson, and Huawei.[70] The 5G example is significant as it shows that, despite clashes with the West, the presumption of Russia's drift toward the Chinese tech sphere has not played out. Even if Chinese tech companies are actively expanding their presence in the Russian market[71] and Huawei extended its investments in R&D in Russia after the United States announced sanctions against the company, a decisive shift to Chinese technologies is anything but certain. Russia's IT sector and its state security services have fundamental security concerns about relying on Chinese IT.[72] Also, Russia is reluctant to solely rely on Chinese companies as they have already been sanctioned by the United States and might be targeted again, leading to a negative spillover effect on Russia itself.

The development of 5G in Russia is facing not only the import substitution problem but also another major obstacle: the availability of the so-called golden band – radio frequencies from 3.4 to 3.8 GHz that are considered to be the most suitable for the development of the network worldwide. For now, Russia's siloviki occupy these frequencies and are not willing to free them up for commercial purposes. As an alternative, Russia's network operators were offered the band from 4.4 to 4.9 GHz. Even if it is also possible to develop a 5G network on this band, equipment costs will be significantly higher and deployment significantly slower under such conditions,[73] much to the chagrin of many investors who see 5G playing a major role in advanced technologies. Consequently, the future of 5G and, with it, Russia's digital economy and competitiveness remains uncertain at best.[74]

Self-Sufficiency in the Software Sector

Russia's position in software development is much stronger than in the hardware sector. Russian IT companies have created their own tools for business, governmental, and private use ranging from cybersecurity and cloud solutions to applications for business management and blockchain voting. When it comes to the government's goal of massively substituting foreign IT with Russian software, however, the domestic sector reveals serious shortcomings.

Among governmental authorities and businesses, there is strong reluctance to decouple from familiar and proven Western technologies.[75] Often, domestic alternatives to foreign IT are lacking, especially in terms of quality. In addition, there are practical hurdles of compatibility. Russian analogues have

67 Janis Kluge, "The Future Has to Wait: 5G in Russia and the Lack of Elite Consensus," *Post-Soviet Affairs* 37 (5), pp. 489–505: <https://doi.org/10.1080/1060586X.2021.1967071> (accessed February 4, 2022).

68 Rostec, "Novikombank and Rostec to Start Syndicated Financing of 5G Technology": <https://rostec.ru/en/news/novikombank-and-rostec-to-start-syndicated-financing-of-5g-technology-/> (accessed February 4, 2022).

69 Nikita Korolev, "Yadro притягивает партнера" [Yadro pulls in a partner], *Kommersant*, November 23, 2021: <https://www.kommersant.ru/doc/5089185> (accessed February 4, 2022).

70 Kovachich, "Who Will Get a Slice of Russia's 5G Pie?" (see note 64).

71 Anastasia Muravyeva and Vasiliy Lemutov, "How Chinese Tech Companies Are Conquering Russia," Carnegie Moscow Center, January 11, 2021: <https://carnegiemoscow.org/commentary/83589> (accessed February 4, 2022).

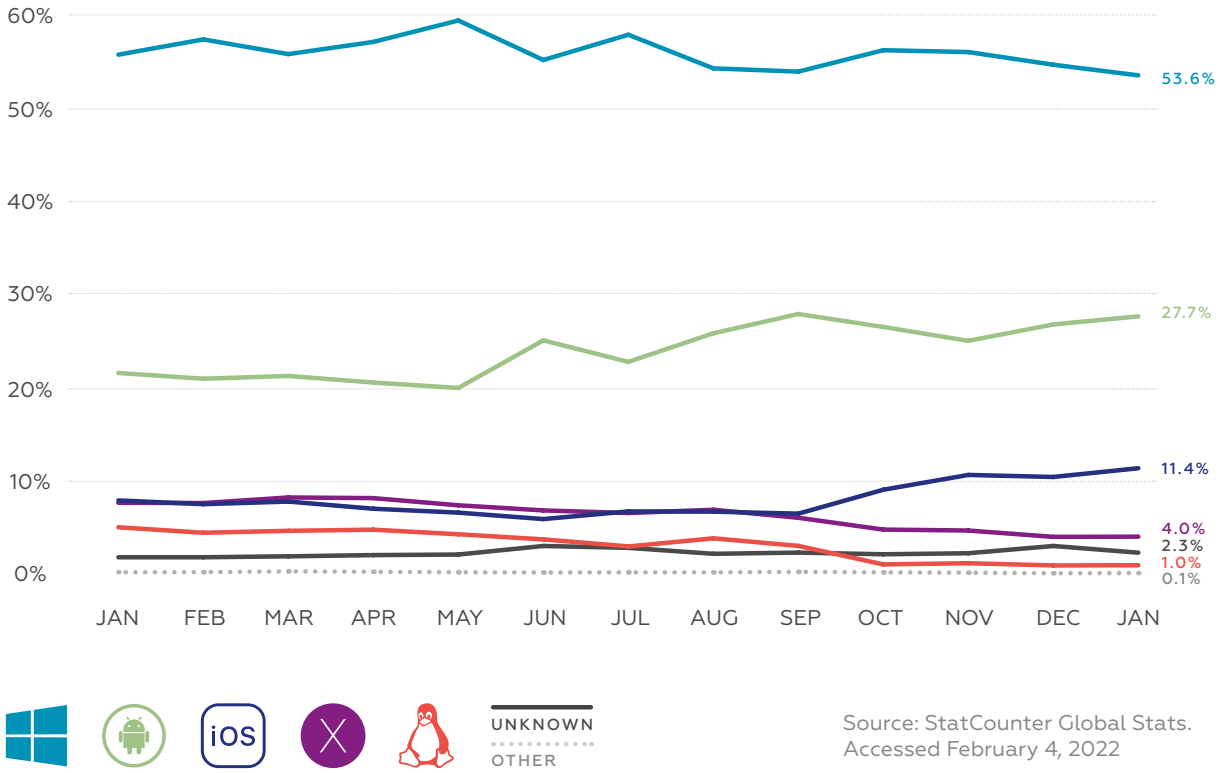
72 Interviews with representatives of the Russian IT sector, academics, and journalists in Moscow in July 2021.

73 Kovachich, "Who Will Get a Slice of Russia's 5G Pie?" (see note 64).

74 Kluge, "The Future Has to Wait" (see note 67).

75 Interviews with representatives of the Russian IT sector, academics, and journalists in Moscow in July 2021.

2 – OPERATING SYSTEM MARKET SHARE OF THE RUSSIAN FEDERATION, JAN 2021 – JAN 2022



Source: StatCounter Global Stats. Accessed February 4, 2022

proven to be poorly compatible both with each other and foreign solutions, for example when it comes to database management systems (DBMS) or operating systems (OS).

Operating Systems

Russia does not have a company that has successfully launched its own widely used operating system (such as Microsoft). For the desktop market and many high-security tasks, for example in many ministries and the military, the operating system Astra Linux is used. Astra Linux is a Debian-based Linux operating system developed by the Russian software company RusBITech. The operating system can run on the ARM, Intel, and Elbrus architecture. There is also a free version of Astra Linux that is available to regular users.

The dominant position for OS on computers in Russia is still occupied by US-based companies. According to market share data, Windows holds more than 53 percent of the market and is an absolute leader; it is followed by Android (28 percent), iOS (11 percent), and OS X (5 percent). Linux only has a market share of one percent (see figure 2).

Therefore, the Russian population is currently all but reliant on foreign technology, and this is unlikely to change in the foreseeable future. To get people to change their operating systems, old systems would have to be banned, which is difficult to achieve politically and economically, or Russian operating systems would have to be better than foreign ones, which would automatically attract Russian users. But no such operating system seems to be currently under development. Moreover, it is unlikely that the country will manage to revolutionize operating systems and overtake leading, well-established competitors.

When it comes to mobile operating systems, two US-based companies command market share: Google (Android) and Apple (iOS). In December 2021, Android

OS held 72 percent of the mobile market in Russia, while iOS held around 27.5 percent.[76] Despite this combined market dominance of 99.5 percent, Russia is trying to develop its own alternatives. The single existing Russian mobile operating system, Aurora, belongs to Rostelecom and is an open source solution on the Linux kernel. Practically speaking, it is a further development of the Sailfish OS developed by the Finnish company Jolla. Aurora is included in the Unified Register of Russian Software, registered by Rospatent, and certified by the Federal Security Service of Russia (FSB). Various applications can be installed on the Aurora platform: browsers, messengers, document management, file storages, etc.[77]

Currently, Aurora OS is installed on many mobile devices of the employees of Russian Railways, the Russian Post Service, and Rostelecom. It was also installed on hundreds of thousands of tablets involved in the All-Russia Population Census in autumn 2021. The mandatory provision of teachers and doctors with Russian tablets based on Aurora OS is currently planned.[78] So most probably, employees of governmental bodies, state-owned companies, and critical infrastructure will soon be obliged to use Aurora on their work smartphones and tablets.

Although Aurora cannot compete with Android and iOS on the free market and could hardly become commercially viable, it is still very likely that the state will continue to create such spaces for the Russian mobile operating system. If Russia's security services continue to see it as a secure solution and an alternative to foreign OS, Aurora has good chances of being implemented in the state sector.

Open Source Software and Repository Hosting Platforms

Like Aurora OS, much of the software that is included in the Unified Register of Russian Software is uploaded onto so-called open source repository hosting services such as GitHub, which belongs to the US-based corporation Microsoft. Smaller businesses are especially dependent on such hosting services. In this case, Russia remains dependent – if not on a certain vendor, then on hosting platforms and access to open source repositories. Disconnection from such platforms could cut Russian developers off from their codes and their audience, which would hinder the development and updates of their products. GitHub, the world's largest host of source code,[79] already blocked access to the accounts of users who accessed its services from Crimea in 2019.[80] Microsoft is required to comply with US export law and was forced to make these restrictions because US sanctions prohibit business relationships with individuals from Crimea. This has meant that many small businesses could no longer access their GitHub accounts – and hence their code – unless they saved it on a backup database.

Since then, the idea of replicating these sites nationally to circumvent such restrictions has arisen in Russia several times. Most recently, Russia's prime minister, Mikhail Mishustin, proposed to launch a domestic analogue version of GitHub.[81] Whether this is at all feasible in practice and if it could have the

ADVANTAGES OF OPEN SOURCE HOSTING

Open source repository hosting services are platforms that let users upload their code and make it available to all users of that platform. Since the code is open source – meaning that it is publicly accessible with the right to redistribute and modify – interested users can create a copy (fork) of the code and amend it. If the original developer approves the new ideas, he or she can merge the forked code into the original file. The advantage for developers of such hosting services is that their code is visible to a broad audience and can be improved by any interested user.

76 Statista, Market share held by mobile operating systems in Russia from January 2012 to December 2021: <https://www.statista.com/statistics/262174/market-share-held-by-mobile-operating-systems-in-russia/> (accessed November 28, 2021).

77 *CNews*, "Сможет ли ОС «Аврора» заменить Android и iOS" [Will the Aurora OS be able to replace Android and iOS], September 10, 2020: <https://mobile.cnews.ru/articles/2020-08-28_smozhet_li_os_avrora_zamenit_android> (accessed November 28, 2021).

78 Ekaterina Kinyakina and Maria Istomina, "Медиков оснастят российскими планшетами" [Medical staff to be equipped with Russian tablets], *Vedomosti*, March 15, 2021: <https://www.vedomosti.ru/technology/articles/2021/03/15/861573-medikov-planshetami> (accessed November 28, 2021).

79 More than 40 million developers worldwide and more than 1.5 million companies, including Apple, Amazon, and Google, use the platform.

80 Rita Liao and Manish Singh, "GitHub confirms it has blocked developers in Iran, Syria, and Crimea," *TechCrunch*, July 29, 2019: <https://techcrunch.com/2019/07/29/github-ban-sanctioned-countries/> (accessed November 28, 2021).

81 *Kommersant*, "Мишустин призвал создать в России аналог GitHub" [Mishustin urged to create an analogue of GitHub in Russia], September 21, 2021: <https://www.kommersant.ru/doc/4996702> (accessed November 28, 2021).

potential of becoming popular is controversial.[82] The incident showed that the fear of being cut off from the outside world, at least in some areas and for some businesses, could be genuine, making a transfer or backup onto Russian systems in line with state interests.

Cloud Computing and Data Sovereignty

For many countries, cloud computing and the data generated by it is of major strategic importance. The use of domestic servers makes enforcing data sovereignty – meaning that data that has been collected or produced in one country falls under local jurisdiction – much easier. One of the aims of data sovereignty is to protect the privacy of users. Many institutions have paid greater attention to it since Edward Snowden's 2013 revelations about the US surveillance system. The European Union, for example, created the General Data Protection Regulation (GDPR) that came into force in 2018 and set rules on how and if data can be transferred outside the EU and the European Economic Area (EEA). In July 2014, Russia passed its data localization law.[83] It forces companies that process the personal data of Russian citizens to do so on Russian soil and to store this data there. In contrast to GDPR, Russia's law aims to grant access to data for security services rather than to protect its citizens' digital rights. However, this access remains limited. To date, many foreign companies do not comply with the law. Prominent examples are Google services and social networks such as Facebook or Instagram. None of the big US internet companies (Meta, Google, or Microsoft) have data centers in Russia.[84] Moscow's courts have fined Google, Facebook, Twitter, and WhatsApp for failing to store the data of Russian users on local servers,[85] but so far this has neither had an effect nor forced the foreign companies to comply with the law.

POSSIBLE IMPLICATIONS OF THE YAROVAYA LAW

In combination with other laws, data localization laws and user data protection can be utilized to perform mass surveillance. In 2016, Russia passed two federal bills known collectively as the "Yarovaya Law." This law forces ISPs and internet services to store user data (messages, phone calls, images, and other data) for up to six months and give the Federal Security Service of Russia (FSB) access to it upon request, even without a court order.[86] Now, if cloud computing servers are on Russian soil, potential surveillance might become even easier. Authorities will have direct access to data centers, giving them far more power in enforcing laws and bans. So far, global companies like Meta are not on the list of services that must comply with the Yarovaya Law. Roskomnadzor has failed to give detailed reasons why not.[87] One assumption, because the data centers of Meta are located abroad, is that enforcing the law is practically impossible. But this could perhaps change if servers were on Russian soil.

Even if large US companies do not yet directly have data centers in Russia, it can be assumed that they will not want to forgo the market in the long term. For Google, Meta, or Microsoft, for example, Russia is already an important market; yet they are currently violating Russian law to some extent. Both cooperation with Russian companies (which we will mention later) and examples from China show that, when the pressure from the authorities becomes too great, companies tend to think economically. For instance, to be able to keep selling its products in China, Apple had to move some of its data onto Chinese soil. Since

82 Julia Stepanova, "Для российского кода откроют хранилище" [A repository will be opened for Russian code], January 20, 2020: <https://www.kommersant.ru/doc/4225365 > (accessed November 28, 2021).

83 Official Internet Portal of Legal Information, Federal law No. 242-FZ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" [On Amendments to Certain Legislative Acts of the Russian Federation to Clarify the Processing of Personal Data in Information and Telecommunication Networks], July 22, 2014: <http://publication.pravo.gov.ru/Document/View/0001201407220042> (accessed December 9, 2021).

84 See Google Data Centers: <https://www.google.com/about/datacenters/locations/> (accessed December 9, 2021).

85 RFE/RL, "Moscow Court Fines Social Media Giants For Refusing To Localize User Data In Russia," August 21, 2021: <https://www.rferl.org/a/russia-fines-user-data/31429573.html> (accessed January 28, 2022).

86 Matthew Newton, "Russian Data Localization Laws: Enriching 'Security' & the Economy," The Henry M. Jackson School of International Studies at the University of Washington, February 28, 2018: <https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/#_ftn13> (accessed February 4, 2022).

87 Andrei Frolov, "Роскомнадзор: Facebook, WhatsApp и Viber нет в списке ОРИ вместе с Telegram, потому что к ним нет претензий от силовиков" [Roskomnadzor: Facebook, WhatsApp and Viber are not on the ORI list along with Telegram, as there are no complaints from law enforcement agencies to them], *VC.ru*, April 19, 2018: <https://vc.ru/flood/36630-roskomnadzor-facebook-whatsapp-i-viber-net-v-spiske-ori-vmeste-s-telegram-potomu-chto-k-nim-net-pretenziy-ot-silovikov> (accessed February 4, 2022).

then, certain iCloud data has been stored on servers there.[88] Apple claims that the data is encrypted and that only Apple has the keys to decrypt it, though this cannot be verified. If Russia were to enforce its data localization law vehemently, it remains to be seen whether Western companies will also give in to the pressure of the state and store their data on Russian soil. Missing out on the Russian market might not be an option for profit-oriented companies like Apple or Google.[89]

Compared to other countries, Russia's current cloud computing market is not particularly large. This is mainly because the use of cloud computing there only started at a late stage. Globally, around 50 percent of companies use cloud-based solutions, while in Russia the figure is just under 20 percent. Nevertheless, the market is growing fast[90] and it warrants taking a closer look at the three sectors that comprise it.

1. *SaaS (Software as a service)*

It is extremely difficult to determine the size of the whole SaaS market in Russia, including foreign companies. SaaS solutions from Microsoft, Meta, or Google are certainly being used in the country, but it is not known by how many users and what revenue these companies generate. In addition, as already mentioned, Google, Meta, and Microsoft do not have any servers in Russia. If a Russian company wants to connect to their cloud services, it must do so via a partner company, which then connects it to one of the data centers abroad.[91] In 2018, the biggest Russian SaaS providers were SKB Kontur (35.6 percent market share), Softline (11.7 percent), and Mango Telekom, now Mango Office (6.7 percent).[92] In 2020, Amazon Web Services (AWS) announced it was partnering with Mail.ru Cloud Services. Until then, the nearest AWS data center was in the German city of Frankfurt/Main. Especially to comply with data localization laws, the partnership makes sense for international and national AWS customers having business with or in Russia. Exact information about the scope of the partnership is not known.[93]

2. *IaaS (Infrastructure as a Service)*

Russia's IaaS market is growing fast. In 2020, it was valued at 100 billion rubles, 19.6 percent more than in 2019. In this market, we encounter the same problem

THREE SERVICE MODELS OF CLOUD COMPUTING

In cloud computing, providers usually offer three different service models:

- **IaaS** (Infrastructure as a Service) provides customers with IT infrastructure, for example servers, that they can rent. Customers then need to manage the software on the servers themselves. While the providers make sure the servers run properly, they usually do not interfere with what customers load onto them.
- **PaaS** (Platform as a Service) provides customers with a platform that enables them to develop applications, for example AI platforms.
- **Saas** (Software as a service) provides finished ready-to-use-software that customers can rent and that fulfills their task with no additional development. For example, email providers or video conferencing platforms are categorized as SaaS.

88 BBC News, "Apple Criticised for Storing Data inside China," May 20, 2021: <https://www.bbc.com/news/technology-57186275> (accessed February 4, 2022). https://vc.ru/flood/36630-roskomnadzor-facebook-whatsapp-i-viber-net-v-spiske-ori-vmeste-s-telegram-potomu-chto-k-nim-net-pretenziy-ot-silovikov

89 Sergey Satanovsky, "Почему IT-гиганты не хотят хранить данные россиян в России" [Why IT-Giants Don't Want to Store Russian Data in Russia], DW, July 2, 2021: <https://www.dw.com/ru/pochemu-it-giganty-ne-hotjat-hranit-dannye-rossijan-v-rossii/a-58137834> (accessed February 4, 2022).

90 Vladimir Kozlov, "Cloud Services Take off in Russia," *bne IntelliNews*, March 19, 2020: <https://www.intellinews.com/cloud-services-take-off-in-russia-178372/> (accessed February 4, 2022).

91 Sarah Lispet, "How to Connect to the Major Public Clouds in Russia," *Megaport*, May 7, 2021: <https://www.megaport.com/blog/how-to-connect-to-cloud-in-russia/> (accessed February 4, 2022).

92 TAdviser, SaaS (Russian market): <https://tadviser.com/index.php/Article:SaaS_(Russian_market)> (accessed February 4, 2022).

93 Rinat Tairov, "Mail.ru и Amazon запустили в России совместный облачный сервис" [Mail.ru and Amazon launched a joint cloud service in Russia], *Forbes*, July 6, 2020: <https://www.forbes.ru/newsroom/biznes/404449-mailru-i-amazon-zapustili-v-rossii-sovmestnyy-oblachnyy-servis> (accessed February 4, 2022).

as in the SaaS sector: Foreign companies also provide these services, and user numbers are not published. What is known, however, is that Russian companies such as Softline or MTS[94] resell foreign cloud services – belonging in part to the US companies Microsoft Azure, Google Cloud, and AWS – to domestic clients.[95] In 2021, according to data from iKS Consulting, Rostelecom was the biggest IaaS provider in Russia (20.8 percent market share), followed by MTS (11.2 percent), Krok (8.3 percent), Selectel (8.2 percent), and SberCloud (6.2 percent).[96] The latter is part of the state-owned company Sberbank (now Sber), Russia's biggest bank. SberCloud has seen extreme growth and could, according to the projections of iKS Consulting, soon be one the biggest players in the Russian IaaS market.[97] China's Huawei also tried to make a push for the Russian market with its service Huawei Cloud, but, because the company feared further US sanctions, it pulled out and switched to a partner model with SberCloud.[98] This was just one of the factors contributing to that company's rapid growth.

3. *PaaS (Platform as a Service)*

In Russia, the PaaS market is substantially smaller than the SaaS and IaaS sectors. At the end of 2020, it was valued at 2.26 billion rubles. But because its two biggest leaders – SberCloud and Yandex.Cloud – are massively growing, the sector's value increased to 4.4 billion rubles in 2021.[99] Once more, no data on market share in the PaaS sector of foreign companies in Russia is known. As of 2021, Russia was the eleventh largest economy in the world, and many of its companies use cloud computing solutions. Yet, in 2019, the share of Russian players in the global market for cloud computing was less than one per cent.[100] Therefore, it can be assumed that foreign players are crucial for business and people in Russia.

As in other digital fields, Russia is actively pushing its users to utilize domestic cloud services. In June 2021, a document presented to Deputy Prime Minister Dmitry Chernyshenko revealed that Russia is promoting the domestic cloud market for smaller businesses. If the latter use these domestic cloud services, the state will subsidize their costs.[101] In July 2021, Russia's Ministry of Digital Development, Communications, and Mass Media announced that the state system for coordinating information will be moved to the domestic unified cloud platform GosCloud. More and more agencies will be transferred to this single cloud platform. Also, starting in 2024, the use of GosTech, a cloud-based unified platform for the development of public digital services and information systems, will become mandatory for federal and regional authorities. It is being created and operated by Sber.[102]

94 *MTS Blog*, "MTS partners with Microsoft to launch Azure-based cloud service in Russia," August 13, 2018: <http://ir.mts.ru/ir-blog/mts-blog-details/2018/MTS-PARTNERS-WITH-MICROSOFT-TO-LAUNCH-AZURE-BASED-CLOUD-SERVICES-IN-RUSSIA/default.aspx> (accessed February 4, 2022).

95 TAdviser, Infrastructure as a Service, IaaS (Russian market): <https://tadviser.com/index.php/Article:Infrastructure_as_a_Service%2C_IaaS_%28Russian_market%29> (accessed February 4, 2022).

96 iKS Consulting, "Российский рынок инфраструктурных облачных сервисов 2021" [Russian IaaS Market 2021]: <http://survey.iksconsulting.ru/page23992645.html> (accessed February 4, 2022).

97 Ibid.

98 Julia Tishina, "Huawei скрылся за облаком Сбербанка" [Huawei hid behind the Sberbank cloud], *Kommersant*, March 3, 2020: <https://www.kommersant.ru/doc/4275431> (accessed February 4, 2022).

99 TAdviser, Infrastructure as a Service (see note 95).

100 Vladimir Kozlov, "Russia's Cloud Service Businesses Are Expanding," *The Moscow Times*, April 18, 2019: <https://www.themoscowtimes.com/2019/04/18/russias-cloud-service-businesses-are-expanding-a65289> (accessed February 4, 2022).

101 *CNews*, "В России придумали способ продвижения отечественных облачных сервисов и инженерного ПО" [Russia has invented a way to promote domestic cloud services and engineering software], June 24, 2021: <https://www.cnews.ru/articles/2021-06-24_v_rossii_pridumali_sposob_prodvizheniya> (accessed February 4, 2022).

102 *CNews*, "«Гостех» станет обязательным с 2024 года" [GosTech will become mandatory from 2024], October 25, 2021: <https://www.cnews.ru/news/top/2021-10-25_gosteh_stanet_obyazatelnym> (accessed February 4, 2022).

RUSSIA'S INTERNATIONAL COMPETITIVENESS: A BUSINESS PERSPECTIVE

To be internationally competitive, Russia's IT sector also needs to focus on global IT trends and other countries rather than solely on the needs of the Russian government and Russian consumers. With around 144 million residents, its domestic market is mid-sized, making it difficult for IT companies to generate scalability. Hence, exports of IT products and services play a crucial role for Russia's developers and Russia's position as a tech power.

Indeed, Russia remains tightly connected to the West not only because of IT imports but also because of the importance of American and European markets for its exported products. For Russian software companies, North America has remained the second most important market after the national market for many years; it makes up 13 percent of total turnover.[103] Europe is next with around 12 percent, followed by the Post-Soviet States with around 7 percent.

Due to political risks that have arisen since Russia's annexation of Crimea in 2014, the country is trying to diversify its export routes and reach out to markets in South and East Asia, the Middle East, and Africa, but their role in Russia's IT industry remains modest for now.[104] It can be expected, however, that Russia's leaders will actively explore these new markets and promote an alternative model of digital "non-alignment" by providing alternative IT solutions in countries with low competition in the software market.

Digital and Innovation Policy

For now, it is unclear how Russia's state-controlled and state-driven digital policy, as well as its ongoing IT import-substitution, will foster the quality of the country's IT and its prospects in the technological race in the long term. It is doubtful that Russian IT companies could become globally competitive under sector development driven by protectionism. On the contrary: artificially favorable conditions for privileged companies and pressure on both foreign companies and independent Russian IT businesses will reduce the country's competitiveness. Moreover, Russia's authoritarian turn and the worsening geopolitical situation will increasingly lead to the retreat of home-grown IT leaders – companies and people – to the West.

In the last few years, the headquarters of several global players, including Nginx, Luxoft, Parallels, and Telegram, were relocated abroad or the companies are being purchased by US[105] or other Western companies.[106] ABBYY just removed most of its products from the Unified Register of Russian Software after transferring the rights to them to its US entities.[107] As far as human capital is concerned, a recent survey revealed that 53 percent of today's IT students would like to leave Russia. What Russia's future IT specialists miss in their own country and look for abroad is a high standard of living; the country to which would most like to move is the United States, followed by the UK and Germany.[108]

These trends will lead to a negative impact on the development of Russia's IT industry and reduce its chances of becoming a technological leader. Aiming to reverse them and keep up in the global technology sphere, Russia's leadership has initiated several strategies[109] for digital and innovation policy. However, their implementation reveals significant problems in achieving the targets and catching up with the leading countries.

103 RUSSOFT Association, *Export of Russian Software Development Industry*, 18-th Annual Survey 2021, p. 63, <https://russoft.org/wp-content/uploads/2021/12/Survey-2021EN.pdf> (accessed February 4, 2022).

104 Ibid.

105 Petr Kharatyan and Angelina Krechetova, "Как россияне продали американцам четыре IT-компании за $10,5 млрд" [How the Russians sold four IT companies to Americans for $10.5 billion], *Vedomosti*, January 16, 2020: <https://www.vedomosti.ru/technology/articles/2020/01/16/820693-amerikantsam-it-kompanii> (accessed February 4, 2022).

106 *CNews*, "Знаменитая российская ИТ-компания Parallels продана в Канаду «без большой прибыли»" [Famous Russian IT company Parallels sold to Canada "without much profit"], December 21, 2018: <https://www.cnews.ru/news/top/2018-12-21_znamenitaya_rossijskaya_itkompaniya_parallels_prodaetsya> (accessed February 4, 2022).

107 TAdviser, "Большинство продуктов Abbyy удалено из реестра отечественного ПО. Права на них переданы в Америку" [Most ABBYY products have been removed from the registry of domestic software. The rights for them were transferred to the United States]: <https://www.tadviser.ru/index.php/Компания:Abbyy_Россия> (accessed February 4, 2022).

108 RBC, "Опрос выявил долю желающих уехать из России студентов ИТ-специальностей" [Survey reveals proportion of IT students willing to leave Russia], November 19, 2021: <https://www.rbc.ru/technology_and_media/19/11/2021/61966d549a7947d03a054ebb> (accessed February 4, 2022).

109 For example, see the Technology Priority Groups of the National Technological Initiative: <https://nti2035.ru/technology/> (accessed February 4, 2022).

One of the main national programs in this field, which is called "Digital Economy," faces serious challenges. It was launched in 2017 and included ambitious plans for the development of the Russian IT industry. Yet, the government has failed to achieve its own performance indicators, postponing deadlines again and again, and cutting the program's budget a number of times.[110] One of the key parts of the Digital Economy program is a federal project on information infrastructure, which also includes the concept of 5G development; it has only reached one of the ten goals set for the second quarter of 2020.[111] There is no clear explanation for this underperformance, but presumably the model of massive state investment is outdated for the needs of a modern digital economy. Instead, such an economy would require functioning innovation ecosystems, developed institutional settings, and a favorable business environment.

Other state strategies did not show better outcomes. Targets for reaching higher shares of Russian high-tech exports within almost ten years have not been reached; in 2020, they had gained less than 1 percent.[112] The level of gross domestic expenditure on research and development (GERD) has not significantly changed in the last decade despite proclaimed goals; in 2020, it only reached a bit over 1 percent.[113] In comparison, GERD in the United States is around 2.7 to 2.8 percent, in China 2 to 2.14 percent, and in Germany 2.8 to 3.1 percent with all rates constantly rising.[114] Investments in innovative development institutes such as Skolkovo and Rosnano hardly paid off for the country's digital development. The share of innovative products – 6 percent – remains at the level of 10 years ago although it was planned to rise to 25 percent by 2020.[115] Russia is 45th out of 132 countries in the Global Innovation Index 2021. In terms of scores, it is almost twice as far behind as the leaders Switzerland, Sweden, and the United States.[116]

When it comes to advanced technologies in transnational patent applications, Russia's share is highest in the field of nanotechnology, followed by security, big data, and robotics.[117] However, in a global context, Russia performs rather poorly and finds itself in catch-up mode. For example, in robotics, Russia is far behind the world's most automated countries Singapore, South Korea, and Japan.[118]

In recent years, artificial intelligence (AI) has been made a high priority by Russia's leadership – mirroring a similar development in many advanced countries. Even if Russia currently has a modest position among world leaders like China and the United States, it is actively developing its technology, regulatory frameworks, and research in this area. Between 2011 and 2019, for example, publications on AI and robotics in Russia grew at 3.6 percent annually, one of the fastest rates in the world.[119]

In October 2019, the country adopted the National Artificial Intelligence Development Strategy for 2020 to 2030 and aims to become one of the world's leaders in AI and robotics. One year later, the biggest players in Russia's AI development – Sberb, Gazprom Neft, Yandex, VK, MTS, and the Russian Direct Investment Fund – signed a code of ethics on AI. It defines general principles and standards for creating, implementing, and using AI technologies.

When it comes to the funding of AI, it is not easy to grasp its precise scope. There are several schemes to foster research and development in AI, but, at the same time, significant cuts have already been made to the budget of the federal AI program.[120] According to

110 *CNews*, "Какими будут российские ИТ после коронавируса" [What Russian IT will be like after the coronavirus], May 29, 2020: <https://www.cnews.ru/reviews/rynok_it_itogi_2019/articles/kakimi_budut_rossijskie_it_posle> (accessed February 4, 2022).

111 Julia Tishina, "В инфраструктуре не сошлись цифры" [The numbers didn't add up in the infrastructure], *Kommersant*, July 28, 2020: <https://www.kommersant.ru/doc/4433373> (accessed February 4, 2022).

112 Dan Medovnikov, "«Стратегия инновационного развития» провалилась" [Innovation Development Strategy Failed], *Vedomosti*, July 22, 2020: <https://www.vedomosti.ru/opinion/articles/2020/07/22/835097-strategiya-innovatsionnogo>(accessed February 4, 2022).

113 Ibid.

114 OECD, *Main Science and Technology Indicators*, Volume 2020 Issue 1, OECD Publishing Paris: <https://read.oecd-ilibrary.org/science-and-technology/main-science-and-technology-indicators/volume-2020/issue-1_e3c3bda6-en#page13> (accessed February 4, 2022).

115 Alexander Sokolov, "Институты развития провалили инновации" [Development institutions failed to innovate], *Vedomosti*, March 2, 2021: <https://www.vedomosti.ru/economics/articles/2021/03/01/859742-instituti-razvitiya> (accessed February 4, 2022).

116 WIPO, Global Innovation Index 2021: <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021_exec.pdf#page=6> (accessed February 4, 2022).

117 Palina Shauchuk, *Report on Russia: technological capacities and key policy measures*, European Commission, June 2021: <https://ati.ec.europa.eu/reports/international-reports/report-russia-technological-capacities-and-key-policy-measures> (accessed February 4, 2022).

118 International Federation of Robotics (IFR), "Robot Race: The World´s Top 10 automated countries," January 27, 2021: <https://ifr.org/ifr-press-releases/news/robot-race-the-worlds-top-10-automated-countries> (accessed February 4, 2022).

119 Leonid Gokhberg and Tatiana Kuznetsova, "Russian Federation," *UNESCO Science Report*, 2021: <https://unesdoc.unesco.org/ark:/48223/pf0000377250> (accessed February 4, 2022).

120 *CNews*, "Финансирование искусственного интеллекта в России урезано на 100 миллиардов" [Funding for artificial intelligence in Russia cut by 100 billion], August, 17, 2020: <https://www.cnews.ru/news/top/2020-08-17_finansirovanie_iskusstvennogo> (accessed February 4, 2022).

a proposed AI road map, Russia will spend 244 billion rubles (about $3.3 billion) on the development of AI through 2024. Some estimates suggest that Russia's fund is far less than those of China and the United States, the global leaders in AI. Still, the amount is comparable to the scope of AI funding in other Western countries such as the UK and Germany.[121]

In Russia's case, it is probably more important to look at who is driving AI development than what the official numbers say. One of the main actors behind Russia's AI strategy and development is a very powerful player – Sberbank, a state-owned bank that is the largest in the country. Sberbank, or simply Sber after having dropped the word "bank" from its logo, no longer positions itself as a mere bank, but rather as a new tech leader in Russia. Under the leadership of its influential president, Herman Gref, it is actively developing its own IT ecosystem around the unprecedented quantity of data it has from its customers, assets, and capital. Sber has invested in services such as food delivery, e-commerce, cloud technology, and digital healthcare, ending up with a very diverse set of digital assets. Doubtless, it realizes the growing importance of AI for future-proofing its business model and is ready to invest into its development. At the same time, it can rely on support from the Russian state, which also sees the potential of AI's dual use nature in possible advantages for the military sector.[122]

The extent to which Russia will be able to reach its goals in the AI race remains to be seen. For now, Russia can hardly be described as a leader in the global context, as it is far behind the tech powers of the United States and China. However, Russia could use the potential of its existing IT sector, scholarly traditions in mathematics, and skilled specialists to develop its own AI solutions for certain niches and regions.

An indicator that Russia might be catching up is that it is moving up in the list of the 500 most powerful computers. Not long ago, Russia had only three supercomputers; today it has seven and is among the top ten leading countries according to the number of supercomputers.[123] Again, in comparison to China and the United States which have 173 and 149 supercomputers respectively, Russia's capacity is rather poor. At the same time, it performs successfully in its league in one of the most promising areas for the future. Moreover, Russia has several domestic actors that are developing supercomputers and have managed to get into the top 500: Yandex, Moscow State University, MTS, and Sber.[124] Recently, Sber launched its second supercomputer, the Christofari Neo, and is catching up with Yandex.[125]

CONCLUSIONS AND RECOMMENDATIONS

Russia's concept of digital sovereignty is a continuation of its long-established understanding of national sovereignty and should therefore be put into a broader context to fully grasp its goals and means. For the declining power, digital sovereignty is merely another form of domestic legitimization and part of the regime's rhetorical positioning as an alternative tech power.

Russia's leadership realized the importance of digital technologies about a decade ago – though it used their potential for regime consolidation rather than the country's economic development. In constant conflict with its own society as well as the West, the regime sees eliminating the country's technological dependencies on the United States and the EU as a way to mitigate its vulnerabilities. Russia's domestic and external tensions are fundamentally linked given that the coun-

121 Nikolai Markotkin and Elena Chernenko, "Developing Artificial Intelligence in Russia: Objectives and Reality," Carnegie Moscow Center, August, 5 2020: <https://carnegiemoscow.org/commentary/82422> (accessed December 20, 2021).

122 Julien Nocetti, "The Outsider: Russia in the race for Artificial Intelligence," IFRI, December 2020: <https://www.ifri.org/sites/default/files/atoms/files/nocetti_russia_artificial_intelligence_2020.pdf> (accessed December 20, 2021).

123 TOP500: <https://www.top500.org/statistics/list/> (accessed December 20, 2021).

124 Aroged, "Seven supercomputers from Russia were among the 500 most powerful systems in the world – the leader is in 19th place," November 15, 2021: <https://www.aroged.com/2021/11/15/seven-supercomputers-from-russia-were-among-the-500-most-powerful-systems-in-the-world-the-leader-is-in-19th-place/> (accessed December 20, 2021).

125 Alexander Marrow, "Russia's Sberbank, enhancing AI offering, unveils second supercomputer," Reuters, November 11, 2021: <https://www.reuters.com/technology/russias-sberbank-enhancing-ai-offering-unveils-second-supercomputer-2021-11-11/> (accessed December 20, 2021).

try's leadership needs the conflict with the West to sustain its legitimacy at home. Yet Russia remains dependent on Western technologies and vendors in several areas, and this dependence cannot be severed without serious damage to the economy and millions of Russian citizens. Still, a scenario in which Russia will be severed from US-based tech cannot be ruled out completely as the gap between state and society is growing – and relations with the West are rapidly growing even more tense.

The domestic and external pressures on the regime also serve as justification for increasing online surveillance and the redistribution of Russia's digital market to privileged actors close to the Kremlin. The siloviki, state-owned companies, and others exploit the vulnerabilities and fears of the Russian regime for their own interests by turning the idea that IT securitization is existentially needed into profit.

Our assessment of the government's IT policy shows that the sovereign internet and the preservation of power are prioritized over technology sovereignty and economic growth. Should this trend continue, it will erode the positive results achieved in Russia's IT sector and harm the digital economy.

Russia's push for a sovereign internet bears enormous costs for civil rights and freedoms. This has already been proven as the state's technological capability to curb public debate has significantly increased in recent years. The result of this policy is an opaque system of censorship that can hardly be monitored externally. This leads not only to a growing gap between state and society, but also silences important voices that share information about Russia to the outside world.

At the same time, the Russian state has openly stepped up pressure on foreign social media companies to enforce cooperation with authorities. Even if foreign companies are still reluctant to follow regulations for censoring content, they have started to accept the new reality and seek compromises with the state. Regardless of their readiness to collaborate, the future of foreign companies dealing with content and information dissemination in Russia looks increasingly dim. While Russian citizens use foreign social media platforms in everyday life, the authorities are gradually pushing these platforms out of the Russian market. Though their loss will leave an enormous gap for Russia's people and economy, the regime's favored networks are likely to benefit from the lack of competitors.

The Russian regime sees social media platforms and IT companies not primarily as profitable businesses, but rather as another tool for controlling society. Consequently, Russian social media are becoming directly controlled by the highest level of the state and transformed into an instrument of security policy. This also applies to Russia's Big Tech business: access to state procurements and internet infrastructure are being gradually transferred to a close group of state-owned companies such as Rostec, Rostelecom, and Sber. This locks out smaller independent IT players that try to develop into the market – which, in turn, limits Russia's ability to innovate even more, accelerating brain drain and the exodus of companies from Russia.

With its sovereign internet policy, Russia is potentially creating a precedent for other countries. Russia is practically establishing an alternative model to China's "golden shield."[126] For many authoritarian regimes, the Russian model could be very attractive. Despite offering less total surveillance than its Chinese counterpart, it has the advantage of being less expensive and technically demanding – meaning it is much more adaptable.

When it comes to technology sovereignty, Russia faces major obstacles in its bid to gain self-sufficiency and become a genuine global tech power. Russia had wanted to join the competition for technological supremacy because of its great power ambitions. However, it overestimated the reality of its IT sector that – despite its potential in certain areas – is not competitive in an overall global context. Many chances for development over the past decade have been deliberately missed for the sake of preserving authoritarian power.

Russia's heavy dependence on Western technologies and IT markets will not disappear anytime soon despite the government's push for IT import substitution. This creates a paradox in Russia's strategy: In order to further develop its digital economy, Russia needs to maintain its dependence. Given the current crisis, however, it is uncertain how Russia wants to continue balancing its digital dependence with its daring foreign policy – and what role China will play.

126 Elizabeth C Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian*, January 29, 2018: <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown> (accessed February 14, 2022).

Recommendations

Against this background, Germany and the EU need their own clear understanding of digital sovereignty. Furthermore, they should clearly define their values and goals in their quest for such sovereignty, especially in terms of data protection, self-determination, market access, and competition. Both Germany and the EU should more actively advocate for an open and free internet; defend digital citizen rights – also on a global level; demand standards from Big Tech and IT companies accordingly; and oppose any state efforts in segmenting the free global internet.

When the West seeks to protect high standards for the digital rights of its citizens from its IT companies, Russian citizens will profit and be somewhat protected as users of those technologies. In addition, the US government, as well as multilateral organizations and civil society, should push global tech companies such as Google and Meta to create a responsible policy specifically for users in Russia to preserve their free exchange of information and freedom of speech. The governments of Western countries should also sharpen export controls and make sure that their technologies are not deployed for surveillance and the restriction of freedoms in Russia.

Germany and the EU need to be more aware of their conditional interest in Russia's digital market and possibilities for cooperation with Russian IT companies. Despite the official rhetoric, Russia is highly dependent on Western IT and needs Western know-how for both its economy and daily use of technologies. Germany and other EU member states should better coordinate their digital policy with the United States and use their leverage to deter Russia if conflict escalates, carefully calibrating the costs for Russia's regime as well as citizens and the economy on both sides.

Moreover, Germany could use existing fora such as the German-Russian Initiative for Digitization of Economy (GRID) to maintain the dialogue with Russian IT businesses and look for opportunities for cooperation and exchange. Germany must better understand the rapidly changing political dynamics in Russia, as well as the increasing securitization of IT, and more realistically assess the risks for its companies operating in the country. At the same time, Germany should use dialogue and involve other EU member states in communicating its position and making proposals for binding regulations in favor of protecting European companies from the possible risks of Russia's sovereign internet.

Finally, while the Russian government tries to artificially reshape existing interconnections, Russia's society, business, and academia genuinely need cooperation with other countries, especially those in the West. Despite the current geopolitical conflict, the EU should not only make use of its science diplomacy, but also extend and further develop its tool kit to deepen cooperation with Russian universities, research centers, and scientists in technological fields – except, of course, where military and dual-use projects are concerned. The EU could use existing projects such as EuRuCAS and CREMLINplus[127] to engage with Russia's IT sector and research centers in areas of common interest. By doing so, it could provide a space for independent research in key areas of advanced technologies. With that, the EU could maintain people-to-people contact between citizens of the EU and Russia – a significant part of the EU's five guiding principles toward the country.

127 EuRuCAS is the European-Russian Centre for cooperation on environmental and climate research in the Arctic and Sub-Arctic while CREMLINplus stands for Connecting Russian and European Measures for Large-scale Research Infrastructures – plus.

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 25 42 31 -0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 1611-7034

Editing Helga Beck

Layout Luise Rombach

Design Concept WeDo

Author picture(s) © DGAP

Federal Foreign Office

This text was written in the framework of a project generously supported by Germany's Federal Foreign Office.