The Impact and Limits of Sanctions on Russia's Telecoms Industry

Kolomychenko, Maria

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

German Council on Foreign Relations

No. 3
March 2024

DGAP ANALYSIS

The Impact and Limits of Sanctions on Russia's Telecoms Industry

Maria Kolomychenko
Visiting Fellow, Center for Order and Governance in Eastern Europe, Russia, and Central Asia

The West responded to Russia's large-scale invasion of Ukraine with unprecedented sanctions targeting its entire tech industry. While the sanctions on the telecoms sector have not had the intended destructive effect on Russia's war machine, they have created significant negative side effects for its populace. Russian propaganda is using them to reinforce its narrative that "the West is fighting Russian citizens, and Vladimir Putin is protecting them."

- **Russia is dealing with Western sanctions and restrictions on its telecommunications sector with the help of gray imports and equipment from little-known brands and by forcing its telecom operators to use domestic hardware.**
- **The transition to domestic and Chinese equipment plays into the hands of the Kremlin in its further development of the "sovereign Runet," which ultimately contributes to the fragmentation of the global internet.**
- **The West's sanctions have caused telecom prices in Russia to rise and plans to build telecommunications networks in remote regions to be cut, hitting the most vulnerable segments of the population. Germany and the EU should not focus on weakening Russia's civilian tech infrastructure, but rather on strengthening the fight against the Kremlin's information hegemony on the Runet.**

Executive Summary

Telecommunications is an industry that is fundamental to the functioning and development of modern states and societies. This fully applies to Russia, which has digitalized its economy and public administration in the last decade – tasks the government made part of the country's domestic policy.* The role of telecommunications for Russia in the context of its war of aggression on Ukraine deserves special mention. To coordinate its actions, the Ministry of Defense of the Russian Federation relies heavily on its telecommunication holding, Voentelecom. It is not surprising that, after the start of Russia's full-scale invasion of Ukraine, some of the first retaliatory sanctions and restrictions by the United States and European Union affected its telecommunications sector.

To get around the EU and US sanctions, as well as restrictions from Western vendors, Russia's telecoms industry started to use three different strategies: the "gray import" or "parallel import" of equipment from top global manufacturers, the search for analogs from second-tier brands from Asia and Israel, and the development of domestic solutions. After researching all these approaches, this author has reached the conclusion that none of them completely meets industry demands.

Russia's telecommunications infrastructure can, however, continue to function in its current state for many years. The industry does not suffer from sanctions so much that it will affect the Russian economy in the near future and thereby hasten the end of Russia's war on Ukraine. The existing infrastructure will allow the Russian economy to function normally for at least the next decade and maybe longer.

At the same time, sanctions in the telecommunications sector have significant side effects of which the EU and its partners should be aware. These sanctions unintentionally hit ordinary Russian citizens, contribute to the further construction of a "sovereign Runet," and, as a result, advance the "Balkanization" of the global Internet. All this leads the Russian segment of the internet to be even more isolated and gives the state greater scope to actively disseminate its propaganda.

While the sanctions policy of the United States and EU on the Russian telecoms sector has little impact on Russia's economy and ending its war in Ukraine, the negative side effects it is already having on Russia's general populace are unwittingly playing into the hands of the Kremlin. This raises the question of whether the United States and EU should even maintain the current sanctions policy in this sector, much less tighten it.

This analysis concludes that the EU should not focus so much on weakening Russia's civilian tech infrastructure but should rather shift its attention to strengthening resistance to the Kremlin's information hegemony on the Runet. It is no accident that the state's full takeover of the Runet and its blocking of all independent media coincided with the start of its war of aggression in Ukraine. Unrestricted access to unbiased information is, in the eyes of the Kremlin, a far more serious issue than difficulties in obtaining the equipment required to keep the country's telecommunications infrastructure in working order. Germany and the EU should consider providing organizational, financial, and advisory support to technical and non-governmental organizations (NGOs) that create services to get around internet censorship.

* Alena Epifanova and Philipp Dietrich, "Russia's Quest for Digital Sovereignty," DGAP, February 21, 2022: https://dgap.org/en/research/publications/russias-quest-digital-sovereignty (last accessed February 21, 2024).

Table of Contents

Introduction

Russia, with its long-term focus on "digitalization," "digital transformation," and "digital economy," uses telecommunications as a foundation for the functioning of the state. Even in the crisis year of 2022, the telecommunications industry in Russia was worth 1.8 trillion rubles (about 24.8 billion euros)[1] or 1.17 percent of the country's GDP. In a survey on e-government done by the United Nations at the end of that year, Russia's development in this area was ranked "very high"; it came in 42nd out of 193 UN member states.[2]

Therefore, it is not surprising that, following the large-scale invasion of Ukraine, the United States and EU imposed large-scale sanctions that particularly affected Russia's telecom industry. The unstable operation of the internet and other communication services could, in theory, undermine Russia's public administration system and economy and disrupt communication between law enforcement agencies and the defense department, which is especially important for a country at war. Sanctioning the telecoms sector could theoretically also destabilize Russian society since a prolonged emergency shutdown of communication is, for ordinary Russian citizens who are accustomed to having high-speed access to the internet, something akin to a harbinger of the Apocalypse.

Fuel was added to the fire by the world's leading manufacturers of telecoms equipment – Cisco, Nokia, and Ericsson – who decided to leave the Russian market of their own volition and eventually even destroyed stocks in their warehouses.[3] This move by major vendors was a big blow to telecom operators in Russia. Succumbing to panic, they finally bought equipment from Cisco, Nokia, and Ericsson for tens of millions of dollars after the start of the war. However, these reserves will only last, at most, until the end of 2024. After that, telecommunication companies will face difficult questions, all of which I explore in this DGAP Analysis: Is it worth continuing to develop Russia's network on the equipment of world leaders, acquiring it through chains of intermediaries? Or is it better to switch to second-tier brands from Asia or Israel? Will the import substitution efforts of the government work, and should one give domestic manufacturers a chance?

I explain how the Russian telecoms sector functions, the reasons behind its total reliance on Western technology, and how it manages to survive under sanctions. I then examine three vectors that the Russian telecommunications industry is currently pursuing in detail:

- The continuation of the purchase of advanced Western telecom equipment using so-called gray or parallel imports
- The search for new suppliers in Asia and the forging of stronger ties with second-tier ("tier 2") suppliers from countries that have not joined export restrictions toward Russia
- Attempts to stimulate the production of domestic telecom equipment and the transition of telecom operators to its use

This analysis lays out why large telecom operators in Russia are not ready to risk their business and experiment with unknown equipment. Instead, they willingly take advantage of the government's permission to "parallel import" the necessary equipment. As a result, despite the withdrawal of global vendors like Cisco, Nokia, and Ericsson from the Russian market, their equipment worth tens of millions of dollars is still supplied to Russia. While these are huge figures in absolute terms, far more is needed to fully meet the industry's needs.

Therefore, Russian telecommunications companies are looking for equipment in China and other Asian countries. They are favored by manufacturers from Israel, some of whom willingly supply their equipment directly to Russia. The Russian government, however, is already forcing telecom operators to switch to existing domestic equipment. At the same time, the Kremlin's bet on import substitution has yet to pay off, and its aim to revive the radio-electronic industry has yet to materialize. With rare exceptions, the Russian authorities have only achieved the mass launch of production lines for the final assembly of quasi-domestic equipment by using imported components and sticking their own label on devices made by Chinese original equipment manufacturers (OEMs).

1 The average weighted rate of the euro to the Russian ruble (EUR/RUB) for 2022 was 72.5259. https://www.audit-it.ru/currency/sr_vz.php (last accessed February 21, 2024).

2 United Nations, "UN E-Government Survey 2022," September 28, 2022 https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022 (last accessed February 21, 2024).

3 TASS, "Cisco destroyed spare parts for equipment in the Russian Federation for 1.9 billion rubles due to the cessation of sales," April 5, 2023: https://tass.ru/ekonomika/17451425 (last accessed February 21, 2024).

As a result, current sanctions have led to an increase in capital expenses by telecom operators, and they are doing their best to shift these costs to end users. Telecom operators have already attempted to raise the traditionally low prices for communications in Russia.[4] Also, operators that had previously been highly competitive suddenly started discussing the joint use of base stations to preserve equipment.[5] Against the backdrop of equipment shortages and problems with raising capital due to the forced withdrawal from major Western exchanges, the future of Russia's telecommunications industry looks uncertain. Consequently, operators are already thinking about abandoning the construction of 5G networks in the country.[6] And these are only the first signs of how Russia's telecoms sector is being impacted by the restrictions of Western countries.

This paper concludes that, despite the issues that have emerged, Russian communications networks can carry on as usual for many years. Russia's telecommunications industry is not adversely affected by sanctions to the extent that they will have an immediate negative impact on the country's economy, which may hasten the end of its war on Ukraine.

At the same time, this DGAP Analysis provides the EU with information on the potential risks and side effects of the West's chosen sanctions policy in the field of telecommunications. These include the possible strengthening of the "sovereign Runet" and, consequently, the further "Balkanization" of the global internet. If the EU wants to avoid such a result, it should consider opposing Vladimir Putin's policies in other ways besides using export controls and economic sanctions. One of the Kremlin's greatest concerns is the unrestricted flow of information on the internet. Therefore, the EU's support of the global tech community in creating tools to counter censorship and content blocking could be crucial to fighting against Russian propaganda and debunking the cult of Vladimir Putin in the eyes of the Russian public.

Sanctions and Export Controls on the Russian Telecoms Sector

After Russia launched its full-scale invasion of Ukraine on February 24, 2022, the United States, EU, and their allies imposed a set of restrictions and sanctions on Russia's high-tech industry, including its telecoms sector. This was followed by the refusal of several global manufacturers to continue working in the country. All the imposed bans can be divided into three broad categories: export controls of high-tech equipment, sanctions against specific telecom operators, and the withdrawal of global telecom equipment vendors from the Russian market.

On the day of the invasion, the administration of US President Joe Biden imposed sanctions aimed at depriving several sectors of the Russian economy of high-tech products that would contribute to its war effort. It was an attempt to stop the supply of such products that could potentially be used to strengthen Russia's military power: semiconductors, computers, telecommunications equipment, information security equipment, lasers, and sensors. The restrictions concerned the supply of high-tech goods manufactured in the United States and products from other countries that use US technology.[7] The announced export control sanctions were the largest ever imposed on a single state and, according to the US Department of Commerce at that time, were supposed to cut Russian imports of high-tech products in half.

4 Marina Tyunyaeva, "Cellular Tariffs May Rise by 10% to 15% in 2023," *Vedomosti*, October 17, 2022: https://www.vedomosti.ru/technology/articles/2022/10/18/946038-tarifi-na-sotovuyu-svyaz-mogut-virasti (last accessed February 21, 2024).

5 TASS, "Ministry of Digital Development of the Russian Federation: Joint Use of Base Stations Will Improve Communication in Settlements," October 7, 2022: https://tass.ru/ekonomika/15675747 (last accessed February 21, 2024).

6 Andrey Stepanov, "Expert: 5G networks have not appeared in Russia and, it seems, will not appear anymore," *Moskovskiy Komsomolets*, August 11, 2022: https://www.mk.ru/economics/2022/08/11/ekspert-seti-5g-v-rossii-ne-poyavilis-i-pokhozhe-uzhe-ne-poyavyatsya.html (last accessed February 21, 2024).

7 The Bureau of Industry and Security, "Implementation of Sanctions Against Russia Under the Export Administration Regulations," February 25, 2022: https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2022/2915-public-display-version-of-new-export-control-measures-on-russia-final-rule-on-public-display-and-effective-2-24-22-scheduled-to-publish-3-3-22/file (last accessed February 21, 2024).

A month later, however, the United States withdrew "messaging software and equipment" from these sanctions.[8] The decision concerned "all ordinary transactions necessary for the receipt or transmission of telecommunications" as well as "the export or re-export, sale, or supply, directly or indirectly, from the United States or by American persons, wherever located, to the Russian Federation," including services, software, hardware (processors and other components), or technologies used for messaging over the internet.

The EU followed a different approach. In its fifth package of sanctions, it imposed a ban on the supply of technologies intended for civilian communication networks to Russia if the state controls them.[9] For Russia, this is painful because government agencies largely control the country's telecommunications industry. In practice, this means that some of Russia's largest telecom operators – at a minimum Rostelecom, Tele2, TransTeleCom, and Tattelecom – can no longer purchase equipment from global vendors like Nokia and Ericsson.

The situation for Russia is further complicated by the fact that targeted sanctions have been imposed on most telecom operators. On the first day of Russia's full-scale invasion of Ukraine, the US Treasury Department announced economic sanctions against Rostelecom, the country's largest fixed-line operator. These restrictions were mainly targeted at prohibiting Rostelecom from raising capital through the US market.[10]

The first operator to be sanctioned by the ban on the purchase of technology was Voentelecom, which not only provides communication services to government agencies and security forces but also develops and repairs communication systems for the military. In June 2022, Voentelecom was included in US and EU sanctions lists.

At the end of February 2023, the US Treasury Department's Office of Foreign Assets Control (OFAC) imposed export restrictions on MegaFon. Althoughthese restrictions do not impose a complete ban on the supply of US equipment and technologies to MegaFon for the provision of communication services, they imply a ban on most commercial transactions with the operator. Ultimately, this complicates MegaFon's processes for purchasing equipment in the same way.[11] In July 2023, Canada imposed sanctions on all four leading mobile operators in Russia: MTS, MegaFon, VimpelCom, and Tele2.[12]

It has become almost impossible for Western vendors to legally supply Russian operators with equipment – despite the absence of a complete ban on the import of telecommunications

The existing sanctions and restrictions have intertwined into such a complex tangle that it has become almost impossible for European and American vendors to legally work with Russian telecom operators and supply them with equipment – despite the absence of a complete ban on the import of telecommunications into Russia. Equally significant are the reputational risks that have emerged for Western companies and complicated their ongoing operations in Russia.

Against this background, Cisco, Nokia, and Ericsson chose to leave the Russian market and announced the

8 The Department of the Treasury, Russia-related General License 25C – Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications, July 14, 2022: https://ofac.treasury.gov/media/924326/download?inline (last accessed February 21, 2024).

9 The European Union, Council Regulation (EU) 2022/576, April 8, 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0576 (last accessed February 21, 2024).

10 US Department of the Treasury, "US Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs," February 24, 2022: https://home.treasury.gov/news/press-releases/jy0608 (last accessed February 21, 2024).

11 US Department of the Treasury, Russian Harmful Foreign Activities Sanctions Regulations 31 CFR part 587, April 12, 2023: https://ofac.treasury.gov/media/931621/download?inline (last accessed February 21, 2024).

12 Government of Canada, "Russian entities connected to Russia's military-industrial complex," July 20, 2023: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-sanctions.aspx (last accessed February 21, 2024).

CONSOLIDATION IN RUSSIA'S TELECOMS INDUSTRY SUPPORTS STATE CONTROL

According to the register of Roskomnadzor, the Federal Service for Supervision of Communications, Information Technology, and Mass Media, there are more than 10,500 companies in Russia that provide mobile services and broadband Internet access. As in many other countries, Russia's telecommunications sector is noticeably consolidated. Together, the five largest companies there occupy 98 percent of the mobile communications market and 57 percent of the broadband market.

The country's largest telecom operator is the state-owned **Rostelecom.** Its main shareholder directly – and through VTB Bank, one of Russia's largest banks – is the Federal Agency for State Property Management. For many years, Rostelecom has held a leading position in the broadband market. It also owns the mobile operator Tele2 Russia (not related to the Swedish Tele2), the country's fifth-largest telecommunications company.

The second largest telecom operator in Russia, based on criteria such as revenue and the number of subscribers, is **MobileTeleSystems (MTS).** It is controlled by the holding company AFK Sistema, which is owned by oligarch Vladimir Yevtushenkov. In third place is **MegaFon,** owned by Russian billionaire Alisher Usmanov's USM Holdings. Fourth is **VimpelCom** (with its brand Beeline), which had been controlled by Veon, the holding of businessmen Mikhail Fridman, Peter Aven, and German Khan, before it was recently sold to top management.

The concentration of the market in the hands of five telecom operators allows the Russian state to effectively control this sector – mainly because these companies are owned by the state or oligarchs close to the Kremlin but also because communications in Russia are strictly regulated by the Federal Security Service (FSB).

Another key player is the state operator **Voentelecom,** which is controlled by the Ministry of Defense. It was explicitly created to "ensure the interests of the state in the field of information security and telecommunications." Voentelecom's main clients are the structures of the Ministry of Defense, Ministry of Internal Affairs, Prosecutor General's Office, and other law enforcement agencies.

termination of business operations there. In practice, this means that Russian companies can no longer conclude new contracts for the supply of equipment from these vendors – at least directly with them and their official distributors. The use of previously purchased equipment is not limited in any way, but its repair and technical support have now become mostly the problems of its buyers.

Those rare Western companies that intend to ethically leave the market yet continue deliveries to Russia or fulfill their obligations under previously signed contracts still cannot freely supply their telecommunications equipment to the country. To not violate the US and EU sanctions, they must request an export license. This is because the supply of high-tech equipment to Russia is now, in principle, the subject of close internal control in the West. Some of these devices also have data encryption functions and can be operated in a dual-use scenario, meaning they can have both civilian and military applications. The supply of such equipment to Russia is now strictly prohibited.

Nokia, for example, claimed in its financial statements that it is "planning a responsible withdrawal from the Russian market for humanitarian reasons and is committed to providing the necessary support to maintain its customers' networks in connection with the withdrawal." This includes "applying for appropriate licenses to provide this support in accordance with the sanctions in force."[13] At the end of 2022, it became known that Nokia was able to obtain only one of the four export licenses it requested. The receipt of the remaining licenses has not been reported to date.

13 LLC Nokia Solutions and Networks, Accounting statements for 2022, April 3, 2023: https://fedresurs.ru/sfactmessage/CBF5CE36F92340D5890426CFE23C3ED5 (last accessed February 21, 2024).

Russia's Tactics

I will now examine the three primary tactics that Russia's telecommunications industry is currently pursuing to mitigate the effects of Western sanctions and restrictions in detail.

THE RISE OF "PARALLEL IMPORTS"

Immediately after the start of the full-scale invasion of Ukraine and the initial Western sanctions on the supply of high-tech equipment to Russia that were announced the same day, domestic telecommunications companies began to hastily purchase large quantities of equipment from foreign vendors for future use.

In March 2022, VimpelCom received a large batch of telecom equipment from Huawei worth about $15 million.[14] In the first quarter of 2022, MTS raised its capital expenditures to 37.3 billion rubles, an increase of almost 30 percent compared to 2021.[15] The company explained this cost increase with the "accelerated purchase of network equipment." According to the Import Genius database, MTS bought a large amount of telecommunications equipment from Ericsson and Huawei.

During the same period, MegaFon spent $42 million on various telecom equipment and components, including many devices from Ericsson and Nokia, as well as from Chinese companies Huawei and ZTE. At this point, direct and full-fledged equipment deliveries to Russia from the largest telecom equipment vendors ended.

The Russian government, aware of the shortage, immediately banned the export of telecom equipment that was already available in the country – along with computers, hard drives, microprocessors, and other devices. This ban was not aimed at consumers; no one prevented Russian citizens from traveling to other countries with computers or routers. Its sole purpose was to prevent the Russian branches of Western firms from taking the equipment stored in their warehouses out of the country and force them to sell it to Russian companies. However, Western vendors chose differently. Cisco Systems, for example, destroyed all its material and technical stocks in Russia that were worth almost 1,864 billion rubles (25.7 million euros).

Consequently, Russia had no choice but to start importing Western equipment in "gray schemes" through chains of reseller companies in other countries, i.e., to allow parallel imports, which the state had previously been fighting. The list of goods that the Ministry of Industry and Trade allows into Russia through parallel imports includes telecom equipment from Cisco, Nokia, Samsung, Hewlett Packard Enterprise (HPE), and others. The government officially allowed companies to purchase and import this equipment into the country in every possible way – with no regard for sanctions, permits, and the copyright holder's consent.[16]

Russia had no choice but to start allowing parallel imports, which the state had previously been fighting

It is not yet known precisely how much telecom equipment has been imported into Russia since then; the Federal Customs Service stopped disclosing statistics on the import of goods into the country after the start of Russia's war on Ukraine. In 2021, about 44.5 million devices worth more than $2.9 billion were imported into Russia using 851761 and 851762 codes, under which various telecom equipment is hidden in customs statistics.[17]

14 Daria Chebakova and Anna Balashova, "Beeline received a batch of equipment from Huawei," RBC, April 18, 2022: https://www.rbc.ru/technology_and_media/18/04/2022/6256f4289a794753c8562684 (last accessed February 21, 2024).

15 Anna Balashova, "MTS made a major purchase of telecom equipment in the first quarter," RBC, May 18, 2022: https://www.rbc.ru/technology_and_media/18/05/2022/628501189a79477d4545dad8 (last accessed February 21, 2024).

16 Order of the Ministry of Industry and Trade of the Russian Federation dated 19.04.2022 No. 1532: http://publication.pravo.gov.ru/Document/View/0001202205060001?index=1 (last accessed February 21, 2024).

17 Brokers Online, Customs Statistics of Foreign Trade of the Russian Federation, 2022: https://brokersonline.ru/search_ts.html (last accessed February 21, 2024).

According to my estimates based on Import Genius data, more than 75,000 batches of various telecom equipment – from both leading brands and second-tier Asian companies – were imported into Russia in 2022. For example, during this time, 7,442 batches of equipment worth $62.7 million were imported into the country under the Cisco trademark. This is only the equipment that the companies declared using this trademark. During the same period, 2,105 batches of Ericsson equipment and 1,298 batches of Nokia equipment were imported to Russia. These devices come to Russia from China, Hong Kong, Turkey, Uzbekistan, and other Asian countries. At the time of this writing, customs statistics for 2023 were not yet available at Import Genius.

Some European distributors also continue to trade with Russia. For example, Glotech, which is registered in the German city of Düsseldorf, shipped 18 batches of Ericsson equipment worth $2.2 million to Russia in 2022, and deliveries continued until the end of that year. In the same period, the Latvian company OTK Group and the German company Akteant supplied significant volumes of equipment to Russia, particularly telecommunications equipment from Siemens.[18] Since the supply of civilian telecommunications equipment to Russia is exempt from sanctions, the work of these European companies is not a violation of any laws and regulations. Instead, it is a matter of moral and ethical choice.

In Russia, meanwhile, there is a growing landscape of distribution companies that earn billions of rubles on parallel imports. I found several previously unknown companies on the market that increased their revenue by thousands of percent in 2022 due to the supply of imported IT and telecom equipment. For example, Lanprint LLC, whose revenue in previous years was at most 500 million rubles (5.7 million euros),[19] ended 2022 with revenue of 36 billion rubles (496.3 million euros) and a net profit of 1.6 billion rubles (22 million euros). According to information on the company's website, it specializes in the wholesale of computer and network equipment. In 2022, Lanprint supplied more than 1,238 batches of equipment from Intel, IBM, Cisco, HP, Dell, etc. to Russia.

Pixel LLC is another company that, in 2022, increased revenue by thousands of percent thanks to parallel imports. The company's website states that it was founded in 2014 and supplies IT and telecommunications equipment to over 1,000 customers. At the same time, until 2022, the company's maximum annual

EFFORTS TO REDUCE DEPENDENCY ON IMPORTED EQUIPMENT

The networks of leading telecom operators in Russia were established in the mid-1990s and built mainly on the equipment of the world's leading manufacturers, i.e., Cisco, Nokia, Ericsson, etc. For decades, the total dependence of this industry on foreign technology was not an issue.

After its annexation of Crimea in 2014, Russia faced large-scale US and EU sanctions for the first time. These sanctions demonstrated to the Kremlin that its aggressive foreign policy leads to unpredictable retaliatory actions that can include the limiting of access to advanced technologies and equipment. As a result, Russian politicians and officials began to openly express displeasure about the fact that communications and data transmission throughout the country – both between ordinary citizens and in the public sector – is carried out through networks that work almost entirely on foreign equipment. In 2014, Vladimir Putin stated that the internet is a "special project of the CIA" and all the data that is transmitted through it "goes through servers that are located in the United States, everything is controlled there."

In 2015, the Russian government instructed relevant ministries to prepare plans for import substitution in the industries under their supervision. The Ministry of Industry and Trade presented a plan stating that, at the time, Russia's dependence on foreign telecom equipment was between 95 and 100 percent, depending on the type of device. According to that plan, the share of foreign telecom equipment in the Russian market was to be reduced by tens of percent by 2020. That plan was never implemented.

18 See Import Genius: https://www.importgenius.com (last accessed February 21, 2024).

19 The average weighted rate of the euro to the Russian ruble (EUR/RUB) for 2021 was 87.1877. https://www.audit-it.ru/currency/sr_vz.php (last accessed February 21, 2024).

revenue was 358 million rubles (4.1 million euros). In 2022, the revenue of Pixel LLC amounted to 8.8 billion rubles (121.3 million euros).[20]

Supplying equipment from the world's top vendors to Russia is now done according to a scheme that resembles this one: the customer company turns to a Russian distributor, and the latter turns to an intermediary abroad. One of these well-known intermediaries is Pixel Devices, a company registered in Hong Kong that supplied over $200 million of electronics to Russia in 2022.[21]

Intermediaries like Pixel Devices place orders with special brokers, i.e., companies that are not official distributors of large vendors but that buy their equipment on the open market. These brokers usually buy leftovers of new and used equipment from end users that they repair and refurbish as necessary before they resell it. The leading companies in this area are from China, and they openly offer a wide selection of refurbished equipment on their websites. Russian electronics suppliers also do not hide the fact that they offer their customers used and refurbished equipment. As a rule, the price of such equipment is significantly lower than that of new products from official distributors. Yet these savings come with the drawback that Russian companies are forced to be content with outdated and previously repaired equipment.

Almost the only way to get new, modern equipment from large vendors is to place an order abroad – not with a broker, but with an official distributor of one of the top manufacturers. In practice, this is a complicated operation to perform. New IT and telecom equipment from leading companies is equipped with GPS trackers, which manufacturers use to monitor compliance with export controls on their equipment. If official distributors import this equipment into Russia, they risk getting many unpleasant questions from manufacturing companies and losing their official status. For this reason, they do not cooperate directly with Russian customers. They are afraid to accept orders from companies without a clear work history, even if those companies are registered outside Russia. When Russian companies do still manage to obtain new equipment from leading vendors, the complex logistics and chain of intermediaries involved result in costs that may be several times more than the manufacturer's suggested retail price (MSRP).

Another way that Russian telecom operators can get their hands on equipment from Cisco, Ericsson, and other brands is through subsidiaries and sister companies located abroad. MTS, for example, operates not only in Russia but also in Armenia and Belarus. Until mid-2023, VimpelCom was part of VEON, a holding that provides communication services in Bangladesh and Pakistan. However, this scheme has its issues. As previously explained, most modern IT and telecom equipment has built-in trackers. In my research, I found that the foreign affiliates of Russian telecom operators thus order and install new equipment for themselves while they send used equipment – which, as a rule, manufacturers no longer track – to the companies related to them in Russia.

Despite such tricks, the volume of necessary telecom equipment supplied does not allow Russian telecom operators to develop the country's infrastructure at the desired pace. Despite Russia's large-scale purchase of equipment after the start of its war on Ukraine, the capital investments of its telecom operators had fallen by 23.7 percent to below 350 billion rubles (4.8 billion euros) at the end of 2022.[22] A comparable reduction in investment in infrastructure had only been seen in 2009, the year after the global financial crisis of 2008. In particular, equipment shortages have resulted in companies reducing the installation of new base stations by more than 60 percent.[23] They now mainly use existing stocks and new supplies to repair existing communication networks.

SUPPORT OF COMPANIES FROM CHINA AND ISRAEL

In the context of a shortage of equipment from European and American vendors, suppliers from China and, to a lesser extent, other Asian countries have become the main hope and support for Russian companies since the war on Ukraine began. This has put companies such as Huawei, one of the world's leading telecom equipment manufacturers, in a difficult situation. Although Huawei calls itself an independent private company, it has an opaque ownership structure and

20 Spark, Financial Statements of JSC Lanprint and JSC Pixel: https://spark-interfax.ru (last accessed February 21, 2024).

21 Steve Stecklow, David Gauthier-Villars, and Maurice Tamman, "The supply chain that keeps tech flowing to Russia," Reuters, December 13, 2022: https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen (last accessed February 21, 2024).

22 Mindigit, Industry Statistics, 2022: https://digital.gov.ru/ru/pages/statistika-otrasli (last accessed February 21, 2024).

23 Timofey Kornev, "Operators have slowed down infrastructure development," *Kommersant*, February 6, 2023: https://www.kommersant.ru/doc/5810667 (last accessed February 21, 2024).

works closely with Chinese authorities.[24] For example, according to documents obtained by the *Washington Post*, Huawei has helped Chinese authorities to create surveillance technology that targets the country's Uyghur minority population.[25]

Beijing takes a restrained position on the issue of the Russian-Ukrainian conflict and is in no hurry to support either of the parties, preferring instead to advocate for peace talks. Against this background, one can expect neither public statements of support for Ukraine from Huawei nor a high-profile withdrawal from the Russian market. Either would inevitably raise questions from the Russian government and become the subject of a political conflict between the People's Republic of China and the Russian Federation. Furthermore, Huawei is in no hurry to leave Russia for economic reasons. According to the most conservative estimates, the company has generated $2 billion in revenue annually in the Russian market in recent years.[26]

At the same time, as the world's top electronics manufacturer, Huawei inevitably suffers reputational losses from continuing to work in Russia. It also risks falling under secondary sanctions from the United States and EU. Consequently, to try to have its cake and eat it too, the Chinese vendor stopped concluding new contracts for supplying equipment that uses American technologies or components to Russia. In addition, leading Russian media outlets cite anonymous sources every few months who claim that Huawei plans to leave Russia. As these oft-repeated plans have yet to come true, it seems as if Huawei supports the reporting of these rumors in the media.

In 2022, Huawei directly shipped about 12,000 batches of various equipment and components to Russia, and distributors and resellers imported another 3,500 batches of the company's devices into the country.[27] The Russian legal entity Huawei Tech Company LLC ended the year with a revenue of 82 billion rubles (1.1 billion euros).

At the end of 2022, another anonymous report stated that Huawei was closing its sales division for telecom equipment and data storage systems in Russia.[28] The reason was the company's fear of falling under secondary sanctions since imported devices could be classified as "dual-use" equipment and used in the public sector. However, Russian distributors continue to advertise these products on their websites and, more importantly, receive declarations of compliance with the requirements of the technical regulations of the Eurasian Economic Union (EAEU). These are mandatory documents that open the way to goods to EAEU countries. As a result, Huawei does not supply to Russia directly, but the equipment is brought to Russia through "parallel imports."

Beyond Huawei, second-tier Asian brands that are less known worldwide continue to ship their equipment to Russia without interruption. In 2022, according to Import Genius statistics, these included Zyxel, TP-Link, D-link, PLANET Technology, Asterfusion, Kyland, Yeastar, New Rock, Digibird, and others. The companies that continue to actively deliver to Russia are not all Asian, however.

Manufacturers from Israel also cooperate with Russian telecom operators. Standing out among them is ECI Telecom (which was absorbed by Ribbon Communication in 2019). This Israeli company has a long-standing relationship with Russia, and, unlike many other vendors, it has never hidden its cooperation with the Russian defense industry. In the late 2000s, ECI Telecom supplied equipment to Voentelecom. At that time, Nikolai Tamodin, then general director of Voentelecom, said that the company had tested equipment from ECI Telecom that used the WiMax standard and was satisfied with the results. Therefore, it planned to continue cooperating with the Israeli vendor and test its LTE equipment.

In 2010, Israeli businessman Shaul Shani, whose companies were then the main shareholder of ECI Telecom, sent an official proposal to Russian President Dmitry Medvedev to sell ECI Telecom to Russia for $2.5 billion.[29] The deal did not happen mainly because, at that time, Russia was in a different political reality and not very interested in investing heavily in

24 Christopher Balding and Donald C. Clarke, "Who Owns Huawei?", May 8, 2019: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669 (last accessed February 21, 2024).

25 Eva Dou, "Documents link Huawei to China's surveillance programs," *Washington Post*, December 14, 2021: https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china (last accessed February 21, 2024).

26 Spark, Financial Statements of JSC Tekhkompaniya Huawei: https://spark-interfax.ru (last accessed February 21, 2024).

27 Import Genius: https://www.importgenius.com (last accessed February 21, 2024).

28 Timofey Kornev and Yulia Tishina, "Huawei behaved uncorporated," *Kommersant*, December 19, 2022: https://www.kommersant.ru/doc/5733165 (last accessed February 21, 2024).

29 Timofey Dzyadko and Eugenia Pismennaya, "Dmitry Medvedev Offered to Buy Israeli Company," *Vedomosti*, December 7, 2010: https://www.vedomosti.ru/technology/articles/2010/12/07/eci_porusski (last accessed February 21, 2024).

the radio-electronic industry. In addition, the head of Russia's Ministry of Communications, Naum Marder, stressed that the ECI Telecom equipment was "not of the latest generation" and expressed doubts that Israeli businessmen would completely transfer technology to Russia if the deal were signed.

After the annexation of Crimea in 2014, when Russia faced the first sanctions and ensuing difficulties in importing high-tech equipment, the owners of ECI Telecom made another attempt to sell the company. In 2015, they negotiated the sale of ECI Telecom to Rostec, a defense holding company headed by Vladimir Putin's close friend Sergei Chemezov.[30] A representative of Rostec traveled to Israel, where he tried to negotiate the purchase of ECI Telecom and the transfer of its production to Russia so that its equipment could be used to create an "integrated communication network" – a special telecommunications infrastructure for the Ministry of Defense and FSB. By that time, however, the value of the transaction had doubled to $5 billion.

In parallel with negotiations on the sale, ECI Telecom tried to gain a foothold in Russia by other means. Also in 2015, the company, through one of its partners in Russia, sought to obtain the status of a producer of equipment of domestic origin from the Ministry of Industry and Trade. This status would have allowed its devices to be purchased by the public sector and defense contractors in Russia. In response, Svetlana Appalonova, a member of the coordinating council for the Innovative Development of the Radio-Electronic Industry of the Ministry of Industry and Trade, stated: "It turned out that no intellectual rights to this equipment belong to the Russian partner. Therefore, it cannot be considered domestic."

These failures did not, however, turn ECI Telecom away from Russia. In 2022, the legal entity ECI Telecom Ltd. directly shipped 671 batches of its equipment and components worth more than $25 million to Russia. According to data from Import Genius, deliveries continued throughout that year. For that period, the revenue of the company's Russian legal entity – LLC "ECI Telecom 2005" –amounted to 662 million rubles (9.1 million euros). The company continued its activities in Russia in 2023. At the beginning of that year, it received several new declarations of compliance with the requirements of the technical regulations of the Eurasian Economic Union on its devices.

Silicom is another Israeli technology company that continues direct deliveries to Russia. It shipped its equipment to Russia throughout 2022, delivering 134 batches worth $11.7 million. It is worth mentioning that the equipment supplied by Silicom is used for the operation and development of the system used by the state to block content on Russia's internet, the Runet. Silicom cannot be unaware of this. Among its Russian buyers are direct contractors of the state tasked with building the "sovereign Runet." Moreover, this fact has been repeatedly covered in the Russian press and discussed by IT professionals on social media.[31]

The availability of alternative equipment from second-tier Israeli and Asian companies certainly helped mitigate the emergency for Russia's telecommunications industry caused by sanctions and tightened export control measures. Clearly, the great advantage of these vendors for Russia is that they are often still ready to supply their equipment to absolutely any buyers – even those who build the "sovereign Runet" or work with Russia's army. However, neither the long-term prospects for cooperation with such Asian and Israeli companies nor the likelihood of the full-fledged development of communication networks based on the equipment of these manufacturers can be realistically assessed at this time.

Due to limited financial capabilities, medium-sized companies cannot compete with established firms like Cisco and Nokia. Not only are their product lines less broad and offer less functionality, but they are also unable to quickly implement the wishes of telecom operators for the customization and refinement of equipment. In addition, telecommunications companies in Russia are suspicious of goods from previously unknown vendors that provide lower rates of uninterrupted operation, offer poor compatibility with existing equipment, and lack an extensive technical support network.

New suppliers will have to earn their place in the Russian market through tests for compliance with the technical requirements of the Eurasian Economic Union, checks by the Federal Service for Technical and Export Control (FSTEC) for the absence of vulnerabilities, and, if the equipment has encryption functions, lengthy processes for obtaining licenses from the FSB. Companies from Asia will have to surmount more than bureaucratic hurdles. They will

30 Maria Kolomychenko, "The Israeli Liaison," *Kommersant*, November 9, 2015: https://www.kommersant.ru/doc/2849815 (last accessed February 21, 2024).

31 Mikhail Klimarev, Dada Lindell, and Andrey Zayakin, "How Russia is preparing to block YouTube and Telegram by purchasing equipment to circumvent sanctions," *The Insider*, October 10, 2023: https://theins.ru/politika/265575 (last accessed February 21, 2024).

THE SPECIAL CASE OF VOENTELECOM

Perhaps the only Russian telecommunications company that was forced to begin an active transition to domestic equipment years ago is Voentelecom. According to Alexander Davydov, its CEO from 2013 to 2017, Voentelecom was "seriously dependent" on the hardware of Cisco, Juniper, Supermicro, HP, Dell, and several other US businesses until 2014. After Russia's annexation of Crimea that year, the Bureau of Industry and Security of the US Department of Commerce added Voentelecom to its list of companies with special export controls. This, according to Davydov, made it difficult for Voentelecom to buy US equipment and forced it to turn its attention to the products of Russian companies.

Due to Voentelecom's secrecy and its relationship to the Russian Ministry of Defense, it is unclear how dependent the company currently is on foreign technology. On multiple occasions, its management has publicly stated that Voentelecom supplies defense and law enforcement agencies with Russian-made communication equipment, which it also uses for its own operations. However, over the past ten years, several of Voentelecom's top managers have been involved in criminal cases due to the sale of foreign telecom equipment to the Ministry of Defense that they had claimed was Russian.

also have to overcome the long-standing prejudices of telecom operators and government agencies in Russia about the security risks related to using this equipment due to alleged backdoors used for espionage and data leaks.

"DOMESTIC" EQUIPMENT MADE OF FOREIGN COMPONENTS

With the start of Russia's war on Ukraine, the first round of sanctions, and the departure of large Western vendors, Russian companies have high hopes for the next round of the government's import substitution policy. As they like to repeat in Russia, "A crisis is a time of opportunity."

The "communication equipment" section of the Russian Register of the Radio-Electronic Industry (REP) features 1,707 different devices from dozens of different companies.[32] However, this large list includes only one base station for LTE networks: R45F produced by GlobalInformService, which is part of the Rostec defense holding. There are no other domestic LTE base stations in Russia. Both the price of the R45F device and volume of its production are unknown. This base station operates in the 450 MHz band, a frequency that most telecom operators in Russia do not use. In this frequency range, the LTE network is only maintained by Tele2 Russia and only in some regions of the country. The fact that even a huge state corporation could not develop an LTE base station that would cover the basic needs of all domestic mobile operators raises big questions.

The situation is slightly better for the routers and switches used by telecom operators. The REP lists the gigabit switches L2 + and L3 from the domestic companies Qtech and Eltex. Yet to meet the needs of Russia's telecom operators, the country should be able to mass produce at least several dozen types of such devices with different characteristics, capabilities, and price ranges.

The rest of the REP consists of highly specialized telecommunications equipment. For example, it lists almost a hundred different types of fire alarms and security alarms that alert owners if intruders enter their property. The registry gives the impression that it is unsuccessfully attempting to show the scope of Russian industry – presenting only an illusion of choice. Studying it carefully reveals that there are only a few truly high-tech products that are produced in Russia.

Despite the shortage of domestic telecom equipment, the Russian government recently made another attempt to forcibly impose import substitution on the country's telecom operators. At the end of 2021, the "big four" mobile operators were completing a 10-year term of licenses for LTE frequencies. The State Commission on Radio Frequencies (SCRF) extended them with one important condition: as of January 2023, they were obligated to use only domestic equipment in the further deployment of networks of this generation. The harsh reality of the lack of mass production

32 Register of the Radio-Electronic Industry (REP): https://gisp.gov.ru (last accessed February 21, 2024).

of the necessary equipment again shattered such ambitious plans. This deficit is even recognized by government agencies. Amid Russia's war on Ukraine, the Ministry of Industry and Trade issued a new plan for import substitution that states that domestic telecom equipment, depending on its type, only has a share of 5 to 18 percent of the Russian market.[33]

Although the ambitious strategy of the SCRF could not be implemented as quickly as planned, this did not prevent the agency from leveraging it to obtain money from telecom operators for its postponement. Telecommunications companies were forced to sign contracts worth more than 100 billion rubles (1.3 billion euros) with domestic manufacturers of base stations. By 2030, they will have to produce about 75,000 devices and transfer them to operators. Essentially, this scheme will allow the state to shift the burden of financing the development of domestic telecom equipment to commercial companies that are not interested in it. After these contracts were signed, the deadlines for beginning the full transition to domestic telecom equipment were shifted to 2028. The Ministry of Digital Development promised that this process would be "gradual."

The delay of the full transition to domestic telecom equipment does not, however, please Russian manufacturers. In response, they began to lobby for the introduction of protective duties on importing telecom equipment if domestic analogs were available and, simultaneously, for duties on importing electronic components into the country to be reduced to zero. This initiative is not a novelty; a similar proposal was discussed in the Federation Council of the Federal Assembly of the Russian Federation five years ago, but it ended in nothing.

All these proposals and agreements have led to a disappointing result for Russia. Currently, another attempt by the state to impose import substitution on the market is collapsing due to lack of cooperation by businesses. Telecommunications companies are simply not ready to entrust infrastructure that consists of thousands of kilometers of wiring to small equipment manufacturers whose devices have yet to prove themselves on the market. Their move to domestic equipment is further impeded by its low level of technical support, lack of necessary functions, and small production volumes – as well as operators' fears that the vendors may "flame out" and close at any time.

Furthermore, Russian equipment manufacturers do not have experience in developing high-tech telecom equipment, and there is a shortage of engineers and other highly qualified workers. Also, Russian manufacturers prefer to take advantage of the state's current desperation by merely assembling almost finished foreign products rather than making full-fledged investments in their own production lines. Because they have received subsidies and contracts with telecom operators from the state – and they still hope that, as they have lobbied, duties on electronic components will be zeroed – they are not striving to spend time and money on developing domestic products. A striking example of this is the recent attempt by the Ministry of Industry and Trade to tighten the minimum requirements for localization of production, after which almost half of the Russian equipment that had been listed in the REP disappeared from the registry.[34]

At the same time, assembling imported components is far from the worst option for creating "domestic" equipment in Russia. There are repeated examples of local companies simply gluing their own labels onto Chinese technology and selling such "domestic electronics" to clients – even to clients like the Ministry of Defense. The state mostly turns a blind eye, but it cannot do without some demonstrative reprisals. Recently, the director general of Avtomatika, a large enterprise within the defense corporation Rostec, was arrested for supplying Chinese equipment that was domestically labeled. The arrest of CEOs of companies at this level is a rarity in Russia.[35]

Despite the challenging circumstances in which Russian industry currently finds itself, the state's efforts – to both force telecommunications companies to enter into contracts with domestic equipment manufacturers and only issue those companies frequencies if they build their networks on Russian hardware – will slowly lead to migration to domestic technologies in the near future. This will eventually give the Kremlin even more control over the Runet.

33 Ministry of Industry and Trade of the Russian Federation, "Action Plan for Import Substitution in the Radio-Electronic Industry of the Russian Federation until 2024," August 26, 2022: https://bod.frprf.ru/public/documents/plan-po-importozameshheniyu-v-radioehlektronnojj-promyshlennosti (last accessed February 21, 2024).

34 Timofey Kornev and Nikita Korolev, "Electronics Have Fallen Out of the Register," *Kommersant*, April 10, 2023: https://www.kommersant.ru/doc/5925670 (last accessed February 21, 2024).

35 Interfax, "CEO of Avtomatika concern arrested in fraud case," June 30, 2023: https://www.interfax.ru/moscow/909669 (last accessed February 21, 2024).

Further Development of the Runet

In the face of sanctions, the construction of new-generation communication networks in Russia has been paused. Telecom operators are focused on "survival," that is, maintaining the operation of 3G networks and gradually expanding the coverage area of 4G. Plans for constructing 5G networks in the country are constantly being rewritten. The government of the Russian Federation is inclined to publicly maintain the appearance that sanctions impact neither the country's economy as a whole nor its development plans. Consequently, it insists that the construction of 5G networks on domestic equipment will begin as early as this year.[36]

Such deadlines seem unrealistic for several reasons. First, there is no industrial production of domestic 5G telecommunications equipment in Russia. Although the state-owned corporations Rostec and Skoltech have repeatedly announced the creation of domestic 5G base stations, these are only "demonstration models." The purchase of foreign 5G equipment has been complicated by sanctions and the withdrawal of global vendors from the Russian market.

The economic feasibility of launching 5G is an important factor. While the government is prompting telecom operators to build new-generation networks, telecommunications companies are in no hurry to invest hundreds of millions of dollars in new infrastructure. Their revenue has already stagnated in recent years due to low prices and weak subscriber growth caused by the widespread penetration of mobile communications in the country. Plus, end users are happy with 4G networks, and the next generation is primarily designed for devices related to the Internet of Things (IoT) and self-driving vehicles. Behind the scenes, representatives of one of Russia's major telecom operators have said that they do not mind skipping the fifth generation of communications when they can move on to creating 6G networks after they recover from the shock of sanctions. However, the government of the Russian Federation – out of vanity and to prove to the world that Russia can keep up with Western countries in the development of technologies – will not allow telecom operators to abandon 5G. The Ministry of Digital Development recently presented a compromise option that proposes to postpone the launch of the commercial operation of 5G networks to 2030.

Behind the scenes, representatives of one of Russia's major telecom operators have said that they do not mind skipping the fifth generation of communications when they can move on to creating 6G networks after they recover from the shock of sanctions

36 Interfax, "The deployment of 5G networks in the Russian Federation is planned from 2024 at frequencies of 4.4–4.9 GHz," September 6, 2022: https://www.interfax.ru/russia/860848 (last accessed February 21, 2024).

Social Impact

Sanctions on the telecommunications sector are now having a huge effect on the ordinary citizens of Russia. The head of Rostelecom, Mikhail Oseevsky, has stated that, due to problems with the supply of equipment caused by Western sanctions, the volume of its program to "eliminate the digital divide" was halved in 2023. Instead of installing 2,000 base stations, the company only installed 1,000.[37] This means that remote settlements will continue to be left without the internet. The high penetration of communication services in Russia is due to the concentration of a significant part of its population in large cities. At the same time, small settlements in remote regions of Siberia and Kamchatka, where not too many people live, are often cut off from communication services entirely.

The lack of equipment resulting from sanctions and the economic complexities described above led to a bill on the joint use of base stations in sparsely populated regions and along highways.[38] This draft law obliges telecommunications operators that have established base stations in these areas to grant network access to the subscribers of all other telecommunication operators. While forcing shared access is meant to appease end users, large telecommunications operators are not happy about their potential obligation to share equipment with competitors.

As a result, telecom operators have raised their subscription fees to transfer the burden of supplying their equipment and increasing expenses to their customers. The rise in prices, in turn, makes mobile communications and broadband internet less accessible to the most vulnerable of citizens – pensioners and people with low incomes. People in these categories are often represented in Vladimir Putin's "nuclear" political base precisely because they live in an information vacuum. Limited access to communication services leaves them alone with television and thus – because all federal television channels are controlled by the state that provides access to them free of charge – Kremlin propaganda.

Due to the sanctions, some foreign telecom operators have already begun to break roaming agreements with telecommunications companies from Russia. This can leave Russians abroad not only with bank cards that do not work due to the departure of Visa and Mastercard from the country, but also without communications. This does not negatively affect the Kremlin, but it further isolates Russian citizens.

There is a belief in the United States and European Union that the harm sanctions cause to common Russian citizens may serve as a catalyst for public unrest that will bring about the end of the war on Ukraine and even the overthrow of Russia's current political regime. In practice, their effect is the opposite.

Western sanctions against the Russian telecoms industry may also have an unwanted side effect: increased Kremlin control over the Russian segment of the internet and, consequently, accelerated development of the "sovereign Runet"

Kremlin propaganda is actively playing on the fears of Russians, telling them that "Russia is in the ring of enemies," "NATO is getting close to Russia's borders," and "the West is trying to break up Russia." The negative effects that sanctions have on the lives of ordinary people in Russia help to spread the Kremlin's narrative that "the West is fighting Russia and trying

37 TASS, "Rostelecom Reduces Digital Divide Project," May 18, 2022: https://www.interfax.ru/russia/841590 (last accessed February 21, 2024).

38 Mindigit, "The joint use of base stations by operators will improve the quality of communication in small settlements," September 7, 2022: https://digital.gov.ru/ru/events/41940 (last accessed February 21, 2024).

to harm the citizens of the country, and Putin is protecting them." Further tightening sanctions, which have a significant effect on the lives of ordinary people but do not hasten the end of Russia's war on Ukraine, will contribute to expanding the support for Vladimir Putin in society – not the opposite.

If Russia ceases to rely on Western technologies, the Kremlin can start making serious efforts to detach the Runet from the global internet

Western sanctions against the Russian telecommunications industry may also have an unwanted side effect: increased Kremlin control over the Russian segment of the internet and, consequently, accelerated development of the "sovereign Runet." The rapid transition to domestic telecom equipment can give the government even more power over the Runet and improve the work of a domestic content blocking system that is already effective at blocking large social networks, virtual private network (VPN) services, and independent media. Chinese allies, who are currently giving Russia massive supplies of their telecom equipment, can also be of assistance to the Kremlin in improving this content blocking system. In recent years, China and Russia have frequently shared experiences in building a "great firewall."[39]

If Russia ceases to rely on Western technologies, the Kremlin can start making serious efforts to detach the Runet from the global internet. In the past, the Russian Security Council has already worked on creating an independent internet for the sole use of BRICS countries.[40] Given the current political tensions with the West, it may return to this idea. Russia's experiments with using its own encryption and a national Domain Name System (DNS) in late January 2024 resulted in a major incident on the Runet, indicating for certain that its efforts to build its own internet infrastructure that is independent from the West are still ongoing.[41]

Sanctions against the telecommunications industry could, therefore, significantly contribute to the global internet's fragmentation. The EU should keep in mind that "Balkanization" – that is, the fragmentation of the global internet into different geopolitical borders – carries many risks. These include the complete subordination of the internet in each individual country to control by its government and a serious decrease in the reliability, stability, and availability of the global internet.

The Runet has long been on a path to "Balkanization." Over the past ten years, Russia has adopted a large number of laws that help the state to establish control over the country's internet infrastructure and allow it to censor content within the national segment of the internet. Thanks to its Sovereign Internet Law, Russia now has a sophisticated system for blocking web pages and services, a domestic DNS system, and an authority for issuing domestic secure sockets layer (SSL) certificates. Furthermore, Russia has started to hold exercises every year to unplug the country from the global internet, making it clear that the government is working to set up the necessary infrastructure to enable the Runet to run entirely on its own. This was a particularly challenging task to complete when the networks of all telecom operators relied solely on Western technologies. Now, the transition to domestic hardware and equipment from Chinese companies has helped to facilitate the isolation of the Runet from the global Internet.

39 Daniil Belovodyev, Andrei Soshnikov, and Reid Standish, "Exclusive: Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship," RFE/RL, April 5, 2023: https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html (last accessed February 21, 2024).

40 BRICS refers to a bloc of emerging market countries – Brazil, Russia, India, China, South Africa, and more – that seek to challenge a world order dominated by the United States and its Western allies; Maria Kolomychenko, "The Russian Security Council instructed to create an 'independent Internet' for the BRICS countries," RBC, November 28, 2017: https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca (last accessed February 21, 2024).

41 Rossiiskaya Gazeta, "The reason for the failure of the Runet was the imperfection of the DNSSEC software," January 31, 2024: https://rg.ru/2024/01/31/eksperty-prichinoj-sboia-v-rabote-runeta-stalo-nesovershenstvo-programmnogo-obespecheniia-dnssec.html (last accessed February 21, 2024).

Conclusions

If the European Union intends to continue its current sanctions policy, it must take all the risks and side effects associated with them into account, especially those that impact Russian society. Sanctions and export controls by the United States and EU only partially cut off oxygen from the telecommunications industry in Russia. While they make a small impact on its current functionality, they do call its further development – in particular, the introduction of next-generation communication networks – into question.

Access to modern equipment and technologies to support, develop, and expand the country's network infrastructure is severely limited. Tricks such as so-called parallel imports only allow Russia to import some of the necessary equipment in the volumes required. In addition, using intermediaries and complicated logistics results in a significant increase in the final price of already expensive equipment. For Russian telecom operators, whose business has stagnated in recent years, the increase in operating costs is a painful process.

Alternative technical solutions from second-tier companies – mainly from China and other Asian countries, as well as from Israel – offer significant benefits in terms of price, availability, and continuity of supply. At the same time, problems often arise when working with them due to missing functionality, interrupted operation, cybersecurity concerns, and a lack of compatibility with the equipment of world vendors on which existing networks were built. The fact that domestic telecom operators are quite inert and accustomed to relying on equipment from established global manufacturers also plays a role. A year and a half ago, they did not even know about the existence of some Asian brands on which they now have to rely. It is inconceivable that any telecommunications company in Russia would place responsibility for the performance of its network – consisting of thousands of kilometers of cables that serve as the foundation for almost all spheres of the country's economy and public administration – on the equipment of young Asian brands.

The government's policy of import substitution has yet to yield tangible results. In a country that has not produced advanced IT and telecom equipment in recent decades, there is neither a school for training technical specialists in this area nor the necessary production facilities. All electronic components used to assemble domestic equipment are sourced from abroad, making their Russian origin questionable. Only a few Russian companies are ready to invest in the creation of their own unique developments and full-fledged production. Many others are abusing the opportunities that have arisen to capture the market and are only engaged in the final assembly of equipment from imported components or the regluing of Russian labels on Asian OEM equipment.

The problems caused by sanctions are now having a greater impact on society than they are on industry

It is the policy of Russia's leadership to ensure that economic problems do not affect the mood in society and support for the Russian Army's actions in Ukraine. The government of the Russian Federation is in denial and – as it does with other sectoral sanctions – broadcasts a thesis to the public about the absence of their effect on the Russian economy that is not completely true. The Kremlin shifts its need to save face onto commercial companies by not allowing them to talk publicly about their problems. This, in turn, causes an even greater shift of these problems to the population. When telecommunications companies announced the need to raise communication prices at the end of 2022 due to increased equipment costs, the Federal Antimonopoly Service immediately threatened them with an investigation.[42] Nevertheless, as time went on, subscription fees have risen because telecom operators needed to pass on their increased expenses to customers. The authorities have simply turned a blind eye to this.

42 Federal Antimonopoly Service of the Russian Federation, "FAS launches investigation into increase in mobile tariffs by MegaFon and Tele2 operators," December 29, 2022: https://fas.gov.ru/news/32376 (last accessed March 7, 2024).

The future of the telecommunications industry, on which the entire Russian economy relies, does not look dramatic, yet it does not offer grounds for too much optimism either. As detailed above, sanctions create challenges for Russian telecommunication companies related to acquiring the latest equipment and introducing new communication standards. They also have negative financial effects on these companies. The largest private telecom operators in Russia have been traded on stock exchanges in the United States and United Kingdom for many years and have used these markets to raise capital for modernizing and developing their communication networks. Now, restrictions on foreign financing, the small size of Russia's domestic market, and high interest rates on loans have significantly reduced the ability of these companies to raise capital for new investment projects. Although the telecommunication industry in Russia is adapting to this new reality and will continue to function, it will not be competitive anytime soon.

For the Kremlin, the free flow of information in Russia is a much more serious problem than the challenges related to obtaining the equipment needed to maintain the country's telecommunications infrastructure

At the moment, the Russian economy, which uses telecommunications as its circulatory system, does not feel the effect of Western sanctions and restrictions. In theory, some of the problems caused by the sanctions could spell trouble for the industry in the future. Take, for example, the change they have forced from vendors that supply the most modern telecom equipment to those that offer compromise solutions from little-known manufacturers. This shift can result in interruptions to the operation of networks that are critical for most sectors of the economy. A separate danger is represented by vulnerabilities that are, one way or another, inherent to almost all high-tech equipment. When such vulnerabilities cause problems, large vendors release updates and provide technical support at lightning speed. Second-tier companies, as a rule, lack the resources to quickly eliminate errors and vulnerabilities and to prevent their occurrence. Therefore, they are less agile in matters related to the emergency patching of security holes. This could make Russian communication networks more vulnerable to hackers of all kinds, including those used by states for politically motivated attacks.

This analysis does not, however, want to paint an overly dire picture or claim that the problems facing the telecoms sector will eventually lead to the collapse of Russia's economy or the end of its war on Ukraine. Russia has a modern telecommunications infrastructure that is based on advanced Western equipment, hardware inventories, and continuing parallel imports. Thanks to this infrastructure, the Russian economy can continue to operate normally for at least the next ten years, if not longer.

The problems caused by sanctions are now having a greater impact on society than they are on industry. Rising subscription fees, reduced plans to deploy networks in remote regions of Russia, and broken roaming agreements have all become problems that primarily affect ordinary people and contribute to their isolation from the rest of the world. The strengthening of the sovereign Runet, which is taking place against the backdrop of Western sanctions, will further aggravate this process.

Recommendations

The EU can maintain its current sanctions policy in the telecommunications sector to ensure that Western communications equipment is not used for military purposes. Yet it should be aware that doing so will neither hasten the end of Russia's war on Ukraine nor destroy the Russian economy. In one way or another, Russian telecom operators will purchase the equipment they require. They will either employ intricate supply chains or locate a substitute from an Asian supplier.

It is worth noting that, while Russia uses Western equipment from reputable international vendors to build its civilian communication networks, it typically does not use such equipment for military purposes. Due to the Kremlin's concerns about vulnerabilities, backdoors, and "spyware" in such equipment, a separate telecommunications holding company – Voentelecom – was established to meet the needs of the Ministry of Defense. Voentelecom has multiple factories that produce domestic equipment for the Russian military and security forces. Therefore, the West does not need to tighten sanctions against technologies used to construct civilian communications networks.

Given the findings and risks described above, this analysis recommends that the EU focuses its attention not on weakening the technical infrastructure of the Runet, but rather on strengthening the fight against the Kremlin's information hegemony there. The machinery of the Russian state keeps its citizens in an information vacuum with the help of television and other controlled media. The global internet is the only channel for obtaining alternative information from independent sources.

That is why the beginning of Russia's war on Ukraine was marked by a complete takeover of the Runet by the state and its blocking of all independent media. As the White House correctly noted in April 2022, when telecom equipment and messaging software were removed from the US sanctions list, "telecommunications services support the flow of information and access to the internet which provides outside perspectives to the Russian people."[43]

If the United States and European Union are interested in weakening support for Vladimir Putin in Russia and hastening the end of Russia's war on Ukraine, they should join the fight against the widespread blocking of unbiased information on the internet. For the Kremlin, the free flow of information in Russia is a much more serious problem than the challenges related to obtaining the equipment needed to maintain the country's telecommunications infrastructure.

The Kremlin is armed with a new, effective system that allows it to successfully block the content of major Western social networks. A small community of developers is trying to help Russians bypass this blocking by creating services based on technologies such as proxy servers and VPN, but Roskomnadzor immediately blocks the most popular of them.

Technical organizations and NGOs that develop services to bypass internet blocking require financial, advisory, and organizational support from Germany and the EU. The creation and broad distribution of efficient techniques to bypass blocking will make it easier for people to access uncensored content and fight state propaganda – not only in Russia, but also in other countries with authoritarian or dictatorial regimes that aim to restrict information flow.

The EU should also bear in mind that further tightening of the current sanctions policy, which harms the telecommunications infrastructure in Russia, may run counter to the goals and values upheld by the global internet community. After Russia's large-scale invasion of Ukraine in February 2022, the Internet Corporation for Assigned Names and Numbers (ICANN), which maintains the key telecommunications infrastructure of the internet, stressed that it would remain neutral. ICANN has opposed punitive measures and instead supports widespread and unimpeded access to the global internet.

If the EU – and Germany, in particular – stand for the support of civil society and free access to information, they should not consider sanctions and export restrictions as the only way to fight authoritarian and dictatorial regimes. Working to ensure the free dissemination of information around the world and fighting against censorship are tasks that are no less important.

43 The White House, "Fact Sheet: United States, G7 and EU Impose Severe and Immediate Costs on Russia," April 6, 2022: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia (last accessed February 21, 2024).

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 and Ellen Thalmann

Layout Lara Bührer

Design Concept WeDo

Author photo courtesy of the author