Tech Sanctions Against Russia: Turning the West's Assumptions Into Lessons

Epifanova, Alena

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

German Council on Foreign Relations

No. 3
June 2023

DGAP ANALYSIS

Tech Sanctions Against Russia

Turning the West's Assumptions Into Lessons

Alena Epifanova
Research Fellow, Center for Order and Governance in Eastern Europe, Russia, and Central Asia

The West assumed that its unprecedented tech sanctions would be the response to Russia's full-scale invasion of Ukraine that would hurt the country most. While their impact took different routes than expected, Russia has been forced to scale back its goals for technological advancement and become more dependent on third countries than ever. As Russia is preparing to wage a protracted war, the EU must make unity and coordination on tech among its member states and partners its ongoing priority. Implementing the restrictive measures and closing loopholes is essential.

– **The United States, the EU, and their partners have made use of their tech advancement and Russia's dependency to curtail both the country's access to information and communication technologies (ICT) and its future development.**

– **While sanctions and export controls are broad and comprehensive, the number of Western ICT companies that have completely exited the Russian market is surprisingly low.**

– **As Russia opts to use grey imports and unlicensed IT, it becomes more vulnerable and dependent on third countries. China provides a technological lifeline, but it is not ready to risk secondary sanctions. Second-tier Chinese companies are exploiting Russia's market, but Beijing keeps its distance in advanced tech.**

Contents

ACKNOWLEDGEMENTS

The author wishes to thank Kim B. Olsen, Philipp Dietrich, Ansgar Gilster, Maria Kolomychenko, Stefan Meister, Roderick Parkes, Alexandra Prokopenko, and Guntram Wolff for their attentive reviews and valuable comments in support of this DGAP Analysis.

EXECUTIVE SUMMARY

Russia's full-scale invasion of Ukraine on February 24, 2022, was followed by a series of sanctions by primarily Western countries that were supposed to limit Russia's ability to wage war. A significant role in these measures is played by sanctions and export controls related to limiting Russia's access to information and communication technologies (ICT). Given the growing technologization of warfare and digitalization of economies, it was assumed that such restrictive measures would be the most effective ones to curtail an adversary's power. Further, in light of Russia's long-standing dependence on key Western hard- and software, those measures were supposed to hit the country especially hard. Indeed, the sanctions and export controls introduced by the United States, the European Union, and their partners have curtailed Russia's access not only to military and dual use technologies, but also to a wide range of advanced commercial technologies. Moreover, they target a number of Russia's key manufacturers and research institutes, effectively impeding the country's future development and preventing it from collaborating with the international scientific community on emerging tech.

More time is needed before the impact of such comprehensive sanctions can be fully grasped. Yet an initial assessment of the dynamics unleashed by the restrictive measures shows discrepancies between assumptions and real developments that must be considered by the international sanctions coalition in their implementation efforts.

First, the comprehensive set of sanctions and export controls has not prevented most Western tech companies from continuing their business with Russia. Only a minor part of them have completely exited the Russian market. While numerous ICT companies have scaled down their activities or stopped new investments in Russia, their services and products remain available there.

Second, Russia has come to rely on China's support in evading export controls and filling its most urgent tech gaps. On the one hand, China has emerged as a beneficiary of Russia's predicament, and Chinese companies with limited international exposure are actively exploiting its IT market. However, Sino-Russian cooperation has significant limits related to the risk of secondary sanctions for China's big tech and to mutual distrust on issues related to security.

Third, the restrictive measures have become a reality check for Russia's IT – a sector that the government sought to make independent from foreign vendors due to security concerns. The imposed sanctions and export controls have led to more vulnerability in terms of information security and Russia's growing dependence on third countries and unproven tech. The insufficient development of key domestic technologies has forced the state to rely on grey imports of hardware and unlicensed software.

The introduced sanctions and export controls have significantly affected Russia's access to ICT and placed the country's economic and geopolitical standing at risk. However, the success of these measures depends on their implementation. While high-end chips became unavailable for Russia and its telecommunication systems have suffered from the restrictions, loopholes and evasion networks remain in place and undermine the impact of sanctions. The European Union (EU) must prioritize unity and coordination among member states and its partners in implementing the restrictive measures and prevent third countries from helping Russia to evade the sanctions.

Western ICT companies should clearly assess their involvement in facilitating the military power and surveillance capacity of the Russian state and stop their business immediately. At the same time, Western companies that provide internet connectivity and social media platforms should resist the pressure of Vladimir Putin's regime and continue to keep uncensored communication channels open for the Russian people to prevent the Russian state from monopolizing the country's information space and further splintering the global internet.

The EU and its partners must be aware of the dynamics and constraints of the Sino-Russian relationship. Despite its proclaimed goal of a technological partnership and the rapidly growing import of chips and hardware from China, Beijing has no interest in a technologically advanced and globally competitive Russia. Instead, China will only take the opportunity to expand its market into Russia in areas that pose no risks of Western secondary sanctions. In other words, China's own dependency on Western tech seriously limits technological partnership between it and Russia. The EU and its partners should leverage this fact in their implementation of the restrictive measures.

Despite a "no-limits" Sino-Russian partnership in tech being prevented by both the constraints described above and mutual security distrust in emerging technologies, cooperation between China and Russia should not be underestimated by the EU and its partners. Rather, they must be prepared to counter joint efforts to exploit vulnerabilities related to the military, critical infrastructure, and economic espionage. In addition, more sophisticated disinformation campaigns that are coordinated by China and Russia could pose a serious threat and must be prevented.

Given the increasing reliance of Russia on grey imports from third countries to mitigate shortages caused by sanctions, the EU and its partners should closely monitor trade activities and impose restrictions on intermediaries and third countries that violate sanctions. International cooperation among governments, tech companies, investigative journalists, and the expert community is crucial for swiftly uncovering and preventing shipments of sanctioned goods to Russia via third countries.

The early impacts of the restrictive measures toward Russia should be analyzed and the results used to better understand their potential and real dynamics. This knowledge could contribute to establishing a broader framework and policy for regulating advanced technologies that, in turn, could prevent their spread in authoritarian countries.

INTRODUCTION

Since Russia's full-scale invasion of Ukraine on February 24, 2022, the West and its partners have introduced unprecedented tech sanctions and export controls on Russia. These measures are not only hurting Russia today but will also impact it for years to come. The United States, European Union, United Kingdom, and other technologically advanced countries such as Japan and South Korea opted for tech sanctions, assuming they would have a severe impact on Russia's economy and military. Moreover, the restrictive measures were expected to curtail Russian President Vladimir Putin's ability to project power and, as stated by European Commission President Ursula von der Leyen, "cut off Russia's industry from the technologies desperately needed today to build a future."[1]

Indeed, given Russia's high dependency on key Western hard- and software, curtailing access to those technologies both limits Russia's economic and military power and further widens its technological gap to other developed nations. The Russian government proved this was true when it dramatically scaled back the technological advancement goals it once prominently proclaimed. In late 2022, Russia gave up its plan to develop its own internationally competitive advanced tech.[2] Instead of leading in advanced technology by 2030, the state is now forced to manage damage control with the main tool left at its disposal: copying and replicating existing foreign technology.

Despite its ambitious high-tech agenda, good digital infrastructure, and solid human capital, Russia has not established the digital sovereignty it sought. Even if it has performed relatively well in areas such as the software industry and cybersecurity, Russia now lags behind most developed countries.[3] Meanwhile, countries like China are closely observing the effects of Western tech sanctions as part of their own attempts to reduce their vulnerabilities in a fast-developing field with major economic implications.

Against this background, this paper takes stock of the dynamics unleashed by the West's restrictive measures on Russia's access to information and communication technologies (ICT). It tests three assumed impacts of these tools and highlights the real dynamics at play:

First, while technology-related sanctions and export controls have significantly impacted Russia's ability to pursue its strategic goals in technological development, they have not cut the country off from Western ICT completely. In fact, a significant number of foreign firms remain in Russia.

Second, China's readiness to support Russia's IT sector is limited by the high risk of secondary sanctions. True, China supplies Russia with sanctioned electronics, and China's second-tier companies are "backfilling" the void left by the withdrawal of foreign companies. However, Beijing has no interest in making Russia technologically competitive, and Chinese big tech is curtailing its Russian business.

Actors from non-sanctioning third states must be prevented from exporting advanced ICT to Russia

Third, the restrictive measures have led to more vulnerability and a growing dependence of Russia on third countries and unproven tech. As Russia further delays a substantial switch to domestic IT, it relies heavily on "parallel imports" and unlicensed software.

The paper concludes by outlining lessons for improving the effectiveness of the introduced restrictive

1 European Commission, "Statement by President von der Leyen at the joint press conference with NATO Secretary-General Stoltenberg and President Michel," February 24, 2022: https://ec.europa.eu/commission/presscorner/detail/en/statement_22_1332 (accessed May 15, 2023).

2 Venera Petrova and Oleg Sapozhkov, "Мысль с ограничением по высоте полета" [A thought with an altitude restriction], *Kommersant*, April 10, 2023: www.kommersant.ru/doc/5925857 (accessed May 15, 2023).

3 Santtu Lehtinen et al., eds., "Russia's Technological Policy and Knowhow in a Competitive Global Context," June 2, 2022: https://www.fiia.fi/wp-content/uploads/2022/06/russias-technological-policy-and-knowhow-in-a-competitive-global-context.pdf (accessed May 16, 2023).

measures for future use. Only by implementing export controls and sanctions successfully can Putin's Russia be excluded from access to advanced technologies and negative economic developments be exacerbated.

A coordinated approach among leading tech countries is essential. High-tech companies from sanctioning states should stop their business with Russia completely – even if they are only indirectly involved in strategically important tech areas. Also, actors from non-sanctioning third states must be prevented from exporting advanced ICT to Russia. International cooperation among governments, tech companies, and the expert community is crucial for uncovering and preventing the import of controlled ICT goods to Russia. Restrictive measures that aim to prevent China from providing Russia with technological assistance should be based on a better understanding of the dynamics between both countries as well the risks for China's own markets and interests.

RUSSIA'S ISOLATION FROM WESTERN TECHNOLOGIES: EXPORT CONTROL AND SANCTIONS

The goal of the restrictive measures related to information and communication technologies is to curtail Russia's access to advanced technologies and consequently weaken its military and economic power. In the age of high-tech warfare and digitalized economies, this is probably the most powerful tool that exists in geopolitical and geoeconomic confrontation. Indeed, export controls on advanced technologies have become a key part of the response of Western countries to Russia's large-scale invasion of Ukraine. While it has long been common practice to prevent malign actors from getting hold of sensitive military and dual use technologies, these measures are now being used more broadly and additionally to restrict Russia's access to a wide range of advanced commercial technologies. Though the introduced export controls have not been able to immediately halt Western ICT from being used in Russia, they have significantly degraded Russia's technological and economic power and will undermine its geopolitical position for years to come.

Including various countries, jurisdictions, and mechanisms, the scope of the new technological restrictions against Russia is unprecedented. Although the United States has an outstanding position in high-tech and dominates information technologies globally, supply chains of critical components are comprised of several countries around the world. Hence, the effectiveness of export controls and technology-related sanctions always depends on a coalition of countries. The role of the European Union and its member states is crucial in this regard.

Export Control Measures

Restrictions on the export of dual-use goods and technologies from Western countries to Russia can be traced back to 2014[4] when they were introduced after Russia illegally annexed Crimea and started the war in eastern Ukraine. Then, a narrower set of export control measures and sanctions was used. The restricting measures have since been widely expanded and designed to cover further technologies and entities strategically and economically important for Russia. This was first done in response to Russia's recognition of the non-government-controlled areas of the Donetsk and Luhansk oblasts of Ukraine and again after its full-scale invasion on February 24, 2022.

Russia's access to Western ICT has been restricted on several levels. For example, the US Department of Commerce's Bureau of Industry and Security (BIS) obliges American companies to get a license for a wide range of technologies before exporting them to Russia. These include electronics, computers, sensors, lasers, and other technologies used in areas such as telecommunications, information security, navigation, avionics, maritime activities, aerospace, and propulsion.[5] The BIS simultaneously introduced "a policy of denial" for all products from which the Russian government or the Russian defense sector will benefit. A "case-by-case review policy" only allows for a few possible exceptions, for instance for items that ensure flight and maritime safety or support humanitarian needs.

The European Union also regulates dual-use export controls and military export controls. However, because its member states are responsible for licensing exports, it has no similar authority to the BIS.[6] Within the framework of the Common Foreign and Secu-

4 Sanctions against companies involved in exports of dual-use technologies were also imposed before 2014, but their scale was insignificant. For example, sanctions against T-Platforms, a major Russian supercomputer developer, were imposed in 2013 on suspicion of violations of export rules. See: Elena Kiseleva and Vladislav Novy, "Санкции Двойного Назначения" [Dual-Use Sanctions], *Kommersant*, March 20, 2013: https://www.kommersant.ru/doc/2150317 (accessed May 15, 2023).

5 Bureau of Industry and Security, Commerce Control List (CCL): https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl (accessed March 18, 2023).

6 Maria Shagina, "The Role of Export Controls in Managing Emerging Technology," in *The Implications of Emerging Technologies in the Euro-Atlantic Space*, ed. Julia Berghofer et al. (Cham, 2023), pp. 57–72: https://doi.org/10.1007/978-3-031-24673-9_4 (accessed May 15, 2023).

rity Policy (CFSP), the EU jointly decides on export restrictions, but the authorities of member states are responsible for their implementation. In coordination with the United States, the EU has expanded export restrictions on goods that could contribute to the enhancement of Russia's industrial capacities. In its ten sanction packages, the EU has not only imposed export embargos on advanced semiconductors, electronics, software, and any kind of dual-use technology to Russia, but also banned the export of quantum computers and software for the development or use of quantum computers.[7]

The EU decides on export restrictions, but member states are responsible for their implementation

Moreover, the BIS includes in its entity list all Russian and foreign companies that potentially contribute to Russia's military and requires them to obtain a license before shipping certain hard- or software to the country. Since the full-scale invasion started, the entity list has been extended eleven times and now includes more than 450 entities based in Russia.[8] It also lists more than 50 non-Russian entities that are based in Belarus as well as other countries around the world ranging from Iran, Kazakhstan, and China to Luxembourg, Latvia, Switzerland, and the United Kingdom.[9] The EU has also expanded its own entity list several times, currently targeting 506 entities. Its list consists exclusively of Russian and Iranian companies,[10] most of which overlap with the US entity list by the BIS.

The most sweeping control mechanism for technology export is the new Foreign Direct Product Rule (FDPR), which the BIS applied on an entire country for the first time.[11] The rule applies to any exports, re-exports, or transfers to Russia of foreign-produced items that are part of the product groups "Software" and "Technology" in categories 3 through 9 of the Commerce Control List (CCL), i.e., electronics, computers, sensors, lasers, and other technologies used in areas such as telecommunications, information security, navigation, avionics, maritime activities, aerospace, and propulsion. Moreover, the FDPR requires a BIS license if components or technologies listed in the CCL of US origin have been involved in the manufacturing of an item anywhere in the world. Consequently, any foreign goods can fall under US export control if they are manufactured with US equipment, based on US components, or use US technology listed in the CCL. Due to its "general policy of denial," the BIS grants licenses for export or re-export to Russia only under certain circumstances and after a strict case-by-case review. If countries and parties involved in multistep manufacturing processes have knowledge that the item will be destined for Russia, they must undergo the licensing process.[12]

Given that hardly any high-end chips in the world are designed or produced without US software or tools, the American government is effectively stopping Russia from producing virtually any advanced technology. It is not only cutting Russia's military industry off from these important components, but Russia's whole economy.

7 Anna Zanina, "Европа Распечатала Пакет" [Europe unpacked the package], *Kommersant*, April 8, 2022: https://www.kommersant.ru/doc/5303741 (accessed March 6, 2023).

8 The extension of the entity list is continuing as the BIS recently announced. See: BIS, "Commerce Expands and Aligns Restrictions with Allies and Partners and Adds 71 Entities to Entity List in Latest Response to Russia's Invasion of Ukraine," May 19, 2023: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3273-2023-05-19-bis-press-release-russia-rules-and-joint-bis-fincen-alert/file (accessed May 31).

9 Federal Register, "Additions of Entities to the Entity List; Removal of an Entity From the Entity List," December 8, 2022: https://www.federalregister.gov/documents/2022/12/08/2022-26622/additions-of-entities-to-the-entity-list-removal-of-an-entity-from-the-entity-list (accessed March 18, 2023).

10 European Union, Council Regulation (EU) 2023/427, February 25, 2023: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0427&from=EN (accessed May 15, 2023).

11 It also applies specifically to the Russian military and to Belarus. BIS Department of Commerce, "Implementation of Sanctions Against Russia Under the Export Administration Regulations (EAR)," March 3, 2022: https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/2919-87-fr-12226-new-export-control-measures-on-russia-effective-2-24-22-published-3-3-22/file (accessed May 15, 2023).

12 David Mortlock et al., "Sweeping Export Controls on Russia and Belarus Reach New Heights: Novel Foreign Direct Product Rules and Expanded Licensing Requirements," *Willkie Farr & Gallagher LLP*, March 24, 2022: https://www.willkie.com/-/media/files/publications/2022/sweepingexportcontrolsonrussiaandbelarusreachnewhe.pdf?utm_source=mondaq&utm_medium=syndication&utm_term=International-Law&utm_content=articleoriginal&utm_campaign=article (accessed May 15, 2023).

The EU and 36 other leading producer nations – including the United Kingdom, Japan, and South Korea – have joined the United States in committing to impose similar substantial controls. Hence, the United States does not need to apply the FDPR in these countries and impose secondary sanctions if they violate the US law or have less restrictive export controls. Instead, US authorities can benefit from the EU's enforcement support and better coordinate the FDPR with its partners.

So far, Russia is the only country in the world that has been targeted by this strict export control measure. Until 2022, the FDPR had only been applied once – against the telecommunications company Huawei. The Chinese tech giant was cut off from semiconductors and software of US origin, a significant hit that caused serious revenue losses.[13]

Sanctions Lists

In addition to their obligation to participate in the export control measures outlined above, all American individuals and companies are prohibited from doing business with numerous blacklisted businesspeople, companies, and government enterprises from Russia – from leading manufacturers to research institutes. The Specially Designated Nationals and Blocked Persons List, collectively called the "Specially Designated Nationals" (SDN) List, includes persons determined by the US government to threaten national security and foreign policy objectives. The list is maintained by the Office of Foreign Assets Control (OFAC) at the US Department of the Treasury.

Russian nationals and companies are not new targets for restrictions by the United States and EU. In 2014, the US Treasury already blacklisted several Russian businesspeople, companies, and government enterprises. Since Russia's large-scale invasion of Ukraine in 2022, the OFAC has added more than 2,500 individuals, entities, vessels, and aircraft to the SDN List. In parallel, the EU expanded its sanctions list, which prohibits the provision of funding or economic resources to 1,473 individuals and 207 entities from Russia in addition to freezing their assets.[14]

Among the blacklisted entities are leading manufacturers such as Baikal Electronics and the Moscow Centre of SPARC Technologies (MCST). Although both companies are known for developing domestic substitutes for Western technologies, their processors always remained dependent on critical foreign components.[15] Baikal Electronics and MCST are not only on the US entity list, but they are also cut off from European suppliers by the EU's export restrictions on "technology which might contribute to the technological enhancement of Russia's defense and security sector."[16]

Russia's oldest chip company, Mikron, is also targeted by the OFAC. When it comes to manufacturing high-end chips, Mikron is far behind international leaders such as the Taiwan Semiconductor Manufacturing Company (TSMC) or Intel. The company is, however, crucial for Russia's economy as it produces chips used by the national payment system "Mir" in debit and credit cards as well as ID documents.[17]

The OFAC not only includes manufacturers and private persons in its SDN List, but also Russian universities such as the Moscow Institute of Physics and Technology (MFTI) that train specialists in theoretical, experimental, and applied physics; mathematics; and computer science. MFTI has been on the US entity list since November 2021 and was added to the EU list after the beginning of the full-scale invasion.[18] As a result, the university and others like it have lost access to Western suppliers and are no longer able to cooperate with legal and natural persons in the United States or take part in joint conferences. Publishing in American scientific journals has become impossible for scientists from these Russian universities.

Several other countries have introduced similar export controls and technology-related sanctions. The United Kingdom, for example, has significantly ex-

13 Dan Strumpf, "U.S. Restrictions Push Huawei's Revenue Down by Nearly a Third," *The Wall Street Journal*, December 31, 2021: https://www.wsj.com/articles/u-s-restrictions-push-huaweis-revenue-down-by-nearly-a-third-11640934969 (accessed March 18, 2023).

14 Council of the European Union, "EU Sanctions against Russia Explained," n.d.: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/ (accessed March 15, 2023).

15 Alena Epifanova and Philipp Dietrich, "Russia's Quest for Digital Sovereignty," DGAP Analysis No. 1, February 21, 2022: https://dgap.org/en/research/publications/russias-quest-digital-sovereignty (accessed March 1, 2023).

16 Council of the European Union, Council Regulation (EU) 2022/428, March 15, 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0428&from=NL (accessed May 16, 2023).

17 Ramish Zafar, "Russia Funds Largest Chipmaker With 7 Billion Rubles In Aid As Sanctions Bite," *Wccftech.com*, September 7, 2022: https://wccftech.com/russia-funds-largest-chipmaker-with-8-billion-rubles-in-aid-as-sanctions-bite/ (accessed May 16, 2023).

18 Council of the European Union, Council Regulation (EU) 2022/328, February 25, 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0328&qid=1647426657418 (accessed May 29, 2023).

panded the scope of advanced tech regulated by its export control rules and is prohibiting business with numerous Russian individuals and companies.[19] Japan expanded the list of its high-tech products that are banned from being exported to Russia, which includes both quantum computers and spare parts for them.[20] South Korea has controlled the export of "strategic items" to Russia and banned shipments of various semiconductors, computers, sensors, lasers, and other high-tech ICTs. In early 2023, the Korean Ministry of Trade, Industry, and Energy widely expanded its exports ban list by adding 741 items from the chemical, steel, auto, machinery, and quantum computer industries, among others. The total number of banned items is now at 798.[21]

ASSUMPTIONS AND REAL DYNAMICS

Too Little, Too Late: The Self-Sanctioning of Western Companies

Given the unprecedented scope of sanctions and export controls, most Western companies were supposed to leave Russia and stop their business with the country that started a war of aggression in Ukraine. Numerous public announcements by tech giants about their exodus led to high expectations that their withdrawals would multiply the effects of the sanctions. However, a closer look at the actual withdrawals shows that a surprising number of firms have remained in the Russian market and continue to provide ICT to Russia even as the war in Ukraine continues.

Dozens of global IT companies have publicly condemned Russia's war against Ukraine and announced the suspension of their business with Russia. Yet the precise number of companies that have completely stopped doing business in Russia is unclear.[22] While data collected by Yale University shows that more than 1,000 companies have announced that they are curtailing their operations in Russia, not all of them have completely departed from the Russian market. Most firms only suspended operations or scaled down their business.[23] Researchers at the University of St. Gallen and the International Institute for Management Development estimate that less than 9 percent of companies headquartered in the EU and G7 countries – that is, 120 of about 1,400 companies – had divested at least their subsidiaries and assets from Russia by November 2022.[24]

A study by the Kyiv School of Economics (KSE) shows that about 7 percent of companies from 89 countries – that is, 235 of 3,304 companies – have completely exited Russia. Estimations that focus on ICT companies are similar to those related to the overall retreat of foreign brands. According to "Leave Russia," a project affiliated with the KSE, only around 5 percent of foreign IT companies – that is, 10 of 192 companies – have completely exited Russia, meaning that they sold at least a part of their business to a local partner and left the market.[25] Fifty-five percent of these companies have ceased their business or suspended operations in Russia. While another 22 percent have continued business as usual, 17 percent continue operating but have scaled back new projects or paused investments. The trend is similar in other relevant categories such as "Technology and Telecommunication," in which only 3 foreign companies – US-based Lexmark and German-based Elster Group and Deutsche Telekom – completely exited the Russian market.

Data collected by the Yale research group was based on a larger number of ICT companies that also included communication services such as Netflix, Meta, or Radio Free Europe. According to this data, about 34 percent of ICT companies – that is, 91 of 267 companies – have withdrawn from the Russian market while 120 of them suspended services, sales, and shipments to Russia. Another 23 companies from this pool have scaled back new sales and reduced manufacturing but continue honoring existing contracts, while 14 companies are "buying time," staying on the market but not developing their business further. At the same time, 19 companies – mostly based in China – are "digging in" by investing in Russia and providing their services as usual.

19 GOV.UK, "UK sanctions relating to Russia": https://www.gov.uk/government/collections/uk-sanctions-on-russia#full-publication-update-history (accessed May 31, 2023).

20 Laura Keffer, "Япония запрещает экспорт в Россию высокотехнологичного оборудования" [Japan bans exports of high-tech equipment to Russia], *Kommersant*, May 13, 2022: https://www.kommersant.ru/doc/5348814 (accessed May 17, 2023).

21 Yonhap News Agency, "S. Korea to add 741 more items on exports ban list against Russia, Belarus," February 24, 2023: https://en.yna.co.kr/view/AEN20230224005300320 (accessed May 29, 2023).

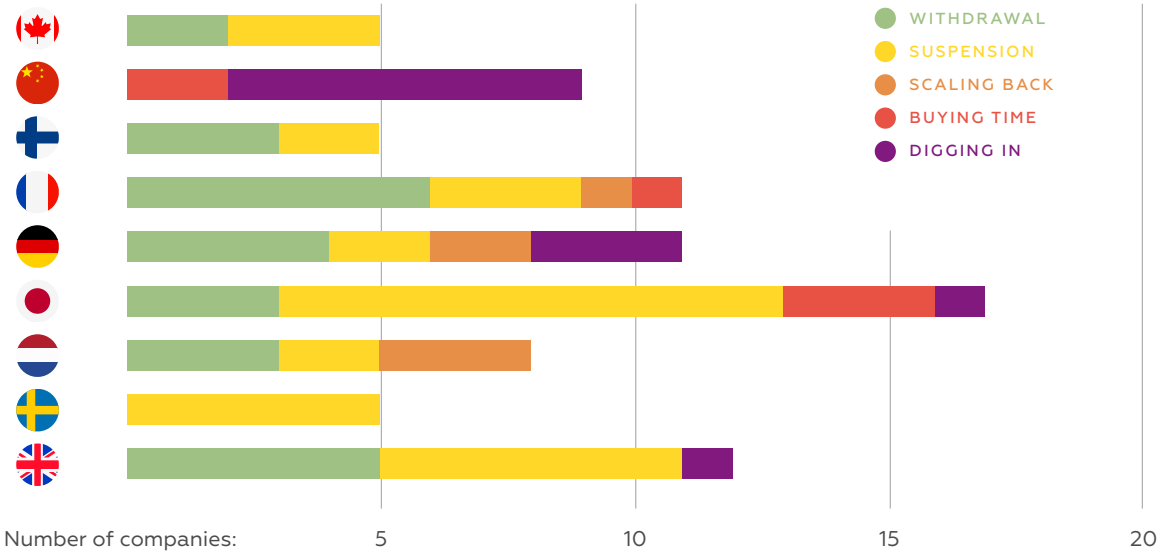
22 Douglas Busvine, "Western Firms Say They're Quitting Russia. Where's the Proof?", *Politico*, February 28, 2023: https://www.politico.eu/article/western-firm-quit-russia-proof-sanctions-war-ukraine/ (accessed March 17, 2023).

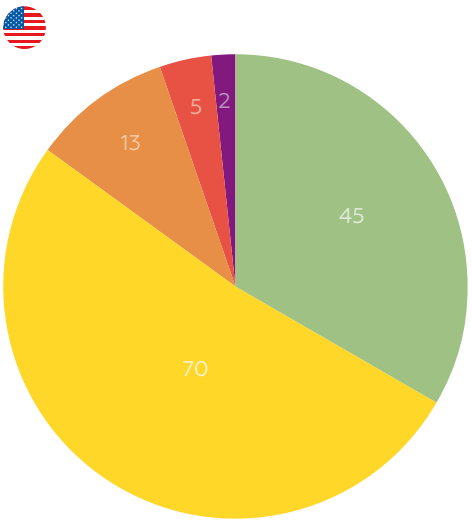
23 Yale School of Management, "Yale CELI List of Companies Leaving and Staying in Russia," n.d.: https://www.yalerussianbusinessretreat.com (accessed March 7, 2023).

24 Simon Evenett and Niccolò Pisani, "Less than Nine Percent of Western Firms Have Divested from Russia," *SSRN*, December 20, 2022: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322502 (accessed May 17, 2023).

25 Leave Russia, n.d.: https://leave-russia.org/bi-analytics?1650483096 (accessed May 29, 2023).

Withdrawal of Foreign ICT Companies from the Russian Market
Many Western Tech Firms Still Remain in the Country





Source: https://www.yalerussianbusinessretreat.com

Nevertheless, a surprising amount of the ICT products and services of foreign companies are still available in Russia and widely used by Russians. Despite numerous public announcements, only a minority of Western companies have completely stopped their business in Russia. Microsoft, for example, halted all new sales but keeps servicing and providing access to the software it has already sold. Not long ago, it started to offer to prolong licenses for foreign companies operating in Russia and not-sanctioned Russian entities.[26] Intel, which proclaimed that it was ending its business in Russia, has recently allowed downloads of its drivers and software inside the country as part of the company's "warranty obligations."[27] Intel is not alone in taking such action. Due to the risk of becoming vulnerable to civil lawsuits, many other companies also cannot cancel the contracts and licenses that they already sold to Russian companies and private users.[28]

Looking at the number of companies that remain in Russia, it is important to differentiate between those technology companies that provide access to independent information and communication channels for the Russian people and those that support the Russian state. US-based companies such as Alphabet, Meta, Twitter, and Cloudflare continue to operate in Russia

26 Timofei Kornev, "Microsoft Предлагает Продлевать" [Microsoft Offers to Extend], *Kommersant*, April 28, 2023: https://www.kommersant.ru/doc/5955078?from=main (accessed May 8, 2023).

27 Paul Alcorn, "Intel Quietly Resumes Russia Support, Unblocks Software Downloads (Updated with Microsoft Comment)," *Tom's Hardware*, January 14, 2023: https://www.tomshardware.com/news/intel-resumes-russia-support (accessed March 2, 2023).

28 J. Scott Marcus et al., "The Decoupling of Russia: Software, Media and Online Services," Bruegel, March 22, 2023: https://www.bruegel.org/blog-post/decoupling-russia-software-media-and-online-services (accessed May 17, 2023).

although they have reduced their commercial activity there. Their availability is of the utmost importance for maintaining the flow of information to people and providing online platforms for news that makes the Russian public aware of the realities of the war. While propaganda channels push pro-Kremlin narratives of the so-called special military operation, the state censorship authorities have blocked the social media platforms Facebook, Instagram, and Twitter; numerous independent media websites; and thousands of webpages seen as undesirable for the regime.[29] After Cloudflare – a provider of content delivery network services, as well as web and cloud cybersecurity services – saw a dramatic increase in requests from Russian networks to worldwide media, it decided not to remove its services as that "would do more harm than good."[30]

Limits of the "No-Limits" Partnership: China's Role in Russia

Until now, Russia has managed to avoid becoming too dependent on China, balancing its tensions with the West and diversifying its cutting-edge imports. Yet under the current sanction regime, Russia has no other choice but to turn to Chinese technologies. This dependence is an opportunity for China. A significant number of imported microchips are currently sold to Russia from China, providing a crucial technological lifeline. Also, Chinese second-tier companies are exploiting Russia's situation and entering a fairly large consumer market with little Western competition. Beijing, however, is cautious enough not to risk secondary sanctions by letting its big tech business continue as usual in Russia.

Russia's war of aggression in Ukraine and the restrictive measures that have been introduced as a result have become a hard reality check for what China and Russia termed a "friendship with no limits" just a couple of weeks before the full-scale invasion.[31] One year later, Vladimir Putin and Xi Jinping claimed to introduce "new models of cooperation" between Russia and China in several areas, including artificial intelligence, the Internet of Things, fifth-generation communication networks, and the digital economy.[32] To what extent such a cooperation will be realized and become more than an empty statement by state leaders remains to be seen. But even as China helps Russia to avoid defeat in Ukraine, the limits of that friendship and cooperation are already being signaled by Beijing.

Western partners are struggling to stop chip imports from China to Russia

In the last year, China has become the Kremlin's crucial partner in evading Western export control measures and enabling Russia to import a significant number of chips. Beijing is the world's largest importer of chips and an important producer of low-end chips. According to trade data, by late 2022, Russia had imported a nearly prewar monthly average of microchips and chip components, more than half of which came from China – a country that has openly condemned Western sanctions.[33] Indeed, Western partners are struggling to stop chip imports from China to Russia that provide a lifeline for Russia's military and its war in Ukraine that urgently needs to be cut off.

At the same time, Chinese companies – particularly those with limited international exposure – are exploiting Russia's situation. They are "backfilling" the void that has been left on the Russian market by the international sanctions coalition and are becoming dominant in telecommunication technologies and

29 OONI, "How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine," February 24, 2023: https://ooni.org/post/2023-russia-a-year-after-the-conflict/ (accessed May 17, 2023).

30 Matthew Prince, "What Cloudflare is doing to keep the Open Internet flowing into Russia and keep attacks from getting out," April 3, 2022: https://blog.cloudflare.com/what-cloudflare-is-doing-to-keep-the-open-internet-flowing-into-russia-and-keep-attacks-from-getting-out/ (accessed May 17, 2023).

31 President of Russia, "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development," February 4, 2022: http://en.kremlin.ru/supplement/5770 (accessed March 29, 2023).

32 Президент России, "Совместное Заявление Российской Федерации и Китайской Народной Республики Об Углублении Отношений Всеобъемлющего Партнёрства и Стратегического Взаимодействия, Вступающих в Новую Эпоху" [Joint Statement of the Russian Federation and the People's Republic of China on Deepening the Relationship of Comprehensive Partnership and Strategic Cooperation Entering a New Era], March 21, 2022: http://www.kremlin.ru/supplement/5920 (accessed March 29, 2023).

33 Ian Talley and Anthony DeBarros, "China Aids Russia's War in Ukraine, Trade Data Shows," *The Wall Street Journal*, February 4, 2023: https://www.wsj.com/articles/china-aids-russias-war-in-ukraine-trade-data-shows-11675466360?mod=article_inline (accessed March 30, 2023).

hardware supplies. In the smartphone segment, the increase in Chinese market share is especially striking: up to 70 percent in quantitative terms in the first quarter of 2023 compared to 50 percent last year.[34] After market leaders Samsung and Apple left Russia, Xiaomi, Realme, Tecno,[35] and other Chinese brands have quickly filled the gap in that niche.

However, even if China is keen to expand its market and might not want Russia to be defeated in Ukraine, its leadership is not interested in making Russia technologically competitive. China might support Russia with urgently needed ICT, but it seems most unlikely that the country would risk secondary sanctions from the United States and its allies for assisting Russia with advanced technologies. While second-tier Chinese companies are backfilling the Russian market, advanced Chinese big tech is curtailing its business with Russia so as not to risk their profitable markets in the EU and US. Moreover, China itself is in a severe technological confrontation with the United States. The rising tensions between the world's two leading powers threaten the shutdown of the flow of Western advanced technologies to Beijing, which could jeopardize China's own progress in producing high-end chips.

The field of telecommunication technologies offers a prime example of China's caution. As previously mentioned, the risk of secondary Western sanctions for Chinese giant Huawei is high. The company already experienced a drop in revenue due to the FDPR imposed by the United States against it in 2020. Now, without public announcements, Huawei has cut the parts of its business in Russia that concern telecommunication equipment for operators and stopped importing base stations for mobile operators.[36] Huawei has also closed its Moscow-based division that was responsible for selling data storage systems and telecommunications equipment to Russia.[37]

Similarly, China's second largest telecom equipment manufacturer, ZTE, which has been present on the Russian market since before the war, remains cautious about its future there. There are some signs that ZTE will reduce its presence in Russia rather than expand it. In 2022, the revenue of ZTE's Russian office decreased by 3.5 times, to 2.8 billion rubles.[38] A financial statement that was published in the database of Russia's Federal Tax Service claims that "there was a significant reduction in the scale of the ZTE's activities due to restrictions caused by sanctions." Indeed, the company has already experienced conflict with American authorities when the United States enacted a trade ban in response to ZTE's violation of sanctions on Iran and North Korea. Even though this ban was later lifted, ZTE is closely monitored by US authorities to ensure its compliance with all US laws and regulations.[39]

Another limitation of China's technological assistance for Russia comes from China's tech confrontation with the United States concerning advanced chips. The global leaders in the market for the most critical tool for the artificial intelligence industry – the graphics processing unit (GPU) – are US-based companies Nvidia and Advanced Micro Devices (AMD). Both suspended their business with Russia shortly after the start of the full-scale invasion of Ukraine, and Nvidia later completely ceased all activities in Russia.[40] Further, the US government introduced export license requirements for explicitly these high-end chips not only for Russia, but also for China. The restriction concerns Nvidia's most advanced products, A100 and H100, and AMD's MI250 chips as well as any future GPUs that can equal the A100 in performance.[41]

GPUs are used in fields such as high-performance computing, storage, and networking capabilities for finance and manufacturing. They also have military

34 Alexander Marrow, "China Smartphone Sales Rise to More than 70% of Russian Market," *Reuters*, April 17, 2023: https://www.reuters.com/technology/china-smartphone-sales-rise-more-than-70-russian-market-2023-04-17/ (accessed May 8, 2023).

35 It should be noted that, apart from Huawei, they all run the mobile operating system Android, which belongs to the US-based Google LLC. This means that the dependency on American technology remains in place.

36 Evgeny Cherkesov, "Huawei закрывает бизнес-подразделение в России и увольняет тысячи сотрудников" [Huawei is closing its business unit in Russia and firing thousands of employees], *Cnews*, December 19, 2022: https://www.cnews.ru/news/top/2022-12-19_huawei_zakryvaet_biznes-podrazdelenie (accessed March 3, 2023).

37 Timofei Kornev and Julia Tishina, "Huawei Повела Себя Некорпоративно" [Huawei did not behave cooperative], *Kommersant*, December 19, 2022: https://www.kommersant.ru/doc/5733165 (accessed March 18, 2023).

38 Tadviser, "ZTE сократила масштабы бизнеса в России из-за санкций, но полностью пока не уходит" [ZTE has scaled back its business in Russia due to sanctions, but it is not leaving completely]: https://www.tadviser.ru/index.php/Компания:ZTE_в_России_(ЗТИ-Связьтехнологии) (accessed May 15, 2023).

39 Claire Ballentine, "U.S. Lifts Ban That Kept ZTE From Doing Business With American Suppliers," *The New York Times*, July 13, 2018: https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html (accessed May 17, 2023).

40 Denny Jacob, "Nvidia Closing Offices in Russia, Ceasing All Activities There," *The Wall Street Journal*, October 3, 2022: https://www.wsj.com/articles/nvidia-closing-offices-in-russia-ceasing-all-activities-there-11664827339 (accessed March 5, 2023).

41 Don Clark and Ana Swanson, "U.S. Restricts Sales of Sophisticated Chips to China and Russia," *The New York Times*, August 31, 2022: https://www.nytimes.com/2022/08/31/technology/gpu-chips-china-russia.html?searchResultPosition=1 (accessed March 5, 2023).

uses. In addition, these high-end chips play a key role in artificial intelligence for machine learning and advancing speech and facial recognition. They are needed to train AI models to quickly analyze large amounts of data, recognize patterns, generate text, and make predictions. Nvidia chips are used in Yandex's supercomputers, for example, to improve the search speed and accuracy of their voice assistant, Alice; the Yandex.Cloud platform; and streaming foreign-language video translation as well as other tasks.

Going beyond this export control, the United States has been expanding its restrictive measures to keep China from producing the most powerful chips domestically. In early 2023, the United States reached an agreement with Japan and the Netherlands to prevent China from acquiring the latest chipmaking equipment.[42] Hence, Russia's future development of AI directly depends on China's capacity to withstand the tech competition from the United States. Replacing Western critical equipment with homegrown alternatives might take years for China. Therefore, Russia's prospects for a broader introduction of AI into its civil and military sectors remain limited.

Apart from China's fear of secondary sanctions, the mutual security concerns of both China and Russia pose an obstacle for an unlimited partnership. According to media reports, senior officials from Russia's Ministry of Digital Development, Communications, and Mass Media (MinTsifry) have raised concerns about the risk of becoming too dependent on Chinese companies and compromising the country's security.[43] Moreover, it is doubtful that Russia's security services and military would allow Chinese companies to dominate the country's telecommunications sector, which was historically balanced between European and Chinese vendors. Discussion around the use of the frequency band that is most suitable for 5G implementation for commercial purposes – 3.4 to 3.8 GHz – is representative of the high securitization of Russia's telecommunications. The fact that those frequencies are occupied by intelligence services and military networks has already been a major stumbling block for Russia's 5G development in recent years.[44]

China has its own security concerns and is not ready to export certain technology to other countries, including its alleged partner Russia. For example, the Chinese government has banned the supply of Loongson processors, which are based on the company's own LoongArch architecture, to Russia.[45] As an original Chinese electronics solution, those processors are used in China's military-industrial complex. Thus, they are recognized as a strategically important technology that is not suitable for export.

However, cooperation between Russia and China and their overlapping interests should be taken seriously. Both countries can strengthen their forces in asymmetric methods of exploiting the vulnerabilities of Western allies by using AI.[46] Despite the significant limits of the alliance between Moscow and Beijing, disinformation campaigns, cyber operations, and economic espionage by the united technological forces of Russia and China pose serious threats for Western societies.

More Vulnerability Instead of Digital Sovereignty

The preoccupation of Russia's leadership with regime security and its high fear of dependence on foreign technologies suggests that the Russian state would switch to domestic technologies and foster import substitution. However, it has decided to bet on opaque import routes from third countries, unproved vendors, and used hardware instead. Rather than using domestic software, the Russian state opts for unlicensed Western software.

The Russian state has softened the shortages caused by the restrictive measures by legalizing grey imports. These so-called parallel imports allow Russian companies to import banned goods without the permission of the rights holders. Imports of ICT have sharply increased not only from countries of the Eurasian Economic Union such as Kazakhstan[47] and Armenia, but

42 Demetri Sevastopulo and Sam Fleming, "Netherlands and Japan join US in restricting chip exports to China," *Financial Times*, January 28, 2023: https://www.ft.com/content/baa27f42-0557-4377-839b-a4f4524cfa20 (accessed March 21, 2023).

43 Alberto Nardelli, "Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech," *Bloomberg*, April 19, 2023: https://www.bloomberg.com/news/articles/2023-04-19/russia-china-worries-set-out-in-private-memo-on-tech-risk (accessed May 17, 2023).

44 Janis Kluge, "The Future Has to Wait: 5G in Russia and the Lack of Elite Consensus," *Post-Soviet Affairs* 37 (5/2021), p. 489–505: https://doi.org/10.1080/1060586X.2021.1967071 (accessed May 18, 2023).

45 Timofei Kornev, "Военно-китайные чипы" [Chinese military chips], *Kommersant*, December 13, 2022: https://www.kommersant.ru/doc/5719932 (accessed May 18, 2023).

46 Katarzyna Zysk, "High Hopes Amid Hard Realities: Defense AI in Russia," DAIO Study 23/11: https://defenseai.eu/wp-content/uploads/2023/02/DAIO_Study2311.pdf (accessed March 21, 2023).

47 Maria Zholobova, Benjamin Bidder, et al., "Kazakhstan Has Become a Pathway for the Supply of Russia's War Machine. Here's How It Works", *IStories*, May 19, 2023: https://istories.media/en/stories/2023/05/19/drones-kz/ (accessed May 29, 2023).

also from Turkey and especially China. These have helped to cover Russia's most urgent needs in electronics. Moreover, Russian intelligence services operating through several front companies have continued to acquire critical technologies from EU companies in Germany and Finland despite sanctions.[48]

Russia is being forced to switch to already used or unproven technologies

However, because third countries are becoming reluctant to export sanctioned technologies to Russia, this approach will be insufficient in the long term. Kazakhstan, for example, is going to introduce the real-time monitoring of the chain of movement of goods to prevent re-export to Russia and avoid secondary sanctions.[49] Also, the United States is constantly expanding its sanctions lists with not only Russian companies, but also intermediaries. For its part, the EU is considering tackling sanctions circumvention by restricting its trade with third countries that violate sanctions. Moreover, for the first time, the EU might even sanction Chinese companies for selling microelectronics that could be used in Russian weapons against Ukraine.[50] Therefore, Russia will need to rely on even more opaque networks to keep supplies flowing into the country.

At the same time, Russia is being forced to switch to already used or unproven technologies from other countries. Its precarious situation is illustrated by the area of mobile networks where Russia is highly dependent on foreign vendors. The entire infrastructure of Russia's telecom operators and existing LTE network is built on foreign hardware: 60 percent consists of European base stations made by Finland's Nokia and Sweden's Ericsson; the remaining 40 percent is built on equipment from Chinese companies Huawei and ZTE.[51] Shortly after the start of the full-scale invasion of Ukraine, both Nokia and Ericsson stopped their business with Russia. Huawei and ZTE are curtailing their business as discussed above.

Russia's existing LTE network has been suffering because of foreign hardware shortages caused by the withdrawal of foreign vendors. According to the estimations of news and analysis firm Telecom Daily, Russian regions have experienced a dramatic drop in mobile internet speeds. In February 2023, mobile internet speeds in all Russian regions except Moscow dropped by around 7 percent in comparison to the previous year. At the same time, Moscow experienced a 32 percent increase in average mobile internet speed.[52] While network equipment is aging and constantly needs modernization, mobile internet traffic in Russia is increasing, and Russian mobile operators are running out of stockpiles. Under these conditions, the operators have been unable to continue the deployment of higher network technology and have moved equipment from small towns and settlements to maintain high speed in the capital and bigger cities.[53]

This is exactly what the Russian operators predicted in spring 2022 when it became clear that the war's end was not imminent and foreign vendors would not soon return to Russia. Once stockpiles are empty, operators have no choice but to cannibalize their networks or, alternatively, import used and dismantled base stations from other countries.[54]

48 Miles Johnson, Max Seddon, and Chris Cook, "Russian Spy Network Smuggles Sensitive EU Tech despite Sanctions," *Financial Times*, May 3, 2023: https://www.ft.com/content/bf892731-2f1c-4c52-b90b-b44ca1911263 (accessed May 8, 2023).

49 Anastasia Stognei and Polina Ivanova, "Kazakhstan to Step up Monitoring of Goods Re-Exported to Russia," *Financial Times*, March 23, 2023: https://www.ft.com/content/b4e8c02a-adb5-4148-9b15-c0cf2845fa0f (accessed May 8, 2023).

50 Andy Bounds, "Brussels Plans Sanctions on Chinese Companies Aiding Russia's War Machine," *Financial Times*, May 8, 2023: https://www.ft.com/content/dc757bea-d7eb-487b-b5d1-1d4360cfb9d5 (accessed May 17, 2023).

51 Evgeny Cherkesov, "Операторов Лишают Поддержки «железа» Nokia, Ericsson и Huawei. Но Выход Найден" [Operators are deprived of support for Nokia, Ericsson, and Huawei hardware. However, there is a way out], *Cnews*, January 30, 2023: https://www.cnews.ru/news/top/2023-01-30_operatorov_lishayut_podderzhki (accessed March 3, 2023).

52 Alexander Marrow, "Russian Internet Speeds Drop on Hardware Shortage, Research Finds," *Reuters*, March 1, 2023: https://www.reuters.com/business/media-telecom/russian-internet-speeds-drop-hardware-shortage-research-finds-2023-03-01/ (accessed May 17, 2023).

53 *The Insider*, "Из-за санкций в России резко упала скорость мобильного интернета. Операторы убирают оборудование из небольших городов и населенных пунктов" [Due to sanctions, mobile Internet speeds have dropped dramatically in Russia. Operators are removing equipment from small towns and villages], June 23, 2022: https://theins.info/news/252521 (accessed March 4, 2023).

54 Julia Melnikova, "Перспектива деградации и монополизации" [A Perspective of Degradation and Monopolization], *Comnews*, April 18, 2022: https://www.comnews.ru/content/219837/2022-04-18/2022-w16/perspektiva-degradacii-i-monopolizacii (accessed March 7, 2023).

Given that European vendors have exited the Russian market and Chinese vendors are decreasing their business, Russia is considering relying on unproven solutions from less known regional vendors. For example, Russian telecom operators have recently started to test second-tier base stations from manufacturers in India, Turkey, and Israel.[55] Installing them, however, would be a major challenge. Not only are the vendors from those countries inexperienced, but new base stations would also need fundamental modification and adaptation. Domestic operators lack expertise in this regard.[56] According to recent media reports, major shipments of telecommunication equipment from Ericsson[57] and Nokia[58] have reached Russia via "parallel import," which suggests that the country still seeks to rely on European solutions. In total, 40,000 base stations will be imported to Russia by an unknown company – equipment estimated to meet the demand of Russia's two major mobile operators for approximately one year. Even if this amount of equipment will not allow Russian operators to maintain network expansion at the previous level and will apparently be used to replace outdated devices, such parallel imports reveal significant limits in curtailing Russia's access to Western tech and must be prevented.

Because Russia's mobile operators have experienced infrastructure shortages for existing networks, it can be expected that they will further consolidate remaining capacities around densely populated cities. This will lead to a patchy network and cause asymmetric internet access around the country; inequality among Moscow, regional centers, and the rest of the country will likely grow. Russia's current fast and affordable mobile internet will probably become a thing of the past. Due to the degradation of its mobile networks, Russia will soon reach the limits of digitalization – another factor that will impede its economy and slow economic growth. While more and more countries will introduce the next generation of cellular networks, Russia will lag further behind.

When it comes to software, the Russian state is ready to take the risk of using unlicensed products by companies from "unfriendly countries" that impose sanctions on Russia. For now, the illegal use of copyrighted objects is to be punished under the Criminal Code of the Russian Federation. However, a new regulation that MinTsifry has been developing is supposed to solve this problem. This planned regulation will grant Russian companies the right to use software against the will of the foreign producer.[59] Practically speaking, Russian companies will be able to continue using foreign software without the consent of the foreign rights holders and not become subject to prosecution if they contribute to a special fund.[60] The government claims that it will use part of this fund to finance preferential IT loans for domestic developers and to support the Russian IT sector. However, because such a policy provides no incentive for switching to the domestic analogues of foreign programs, it will likely further delay the development of Russia's IT industry. Moreover, this measure will lead to significant information security risks for companies and government systems. Despite the increased risk of hacker attacks and data breaches, though, it seems to be the most suitable work-around for Russia's industry given that a switch to domestic analogues is not yet an option. According to MinTsifry, only 20 percent of the software used by Russian companies and industrial enterprises has "adequately mature Russian analogues," and it would take two to three years to fully develop and implement them.[61]

The massive brain drain that occurred in Russia after the outbreak of the war is also a problem. It means that the import substitution, innovation, and ad-

55 Vadim Krasnikov, Timofei Kornev, and Julia Tishina, "Следующая Станция — Индийская" [Next Station – India], *Kommersant*, February 9, 2023: https://www.kommersant.ru/doc/5812512 (accessed March 4, 2023).

56 Ibid.

57 Erdni Kagaltynov, "Отсель ввозить мы будем шведа" [From here we will import a Swede], *Kommersant*, May 3, 2023: https://www.kommersant.ru/doc/5967047 (accessed May 29, 2023).

58 Valery Kodachigov, "Частотная собственность: параллельный импорт базовых станций в РФ удалось наладить" [Frequency ownership: parallel imports of base stations in Russia have been established], *IZ.RU*, May 17, 2023: https://iz.ru/1513557/valerii-kodachigov/chastotnaia-sobstvennost-parallelnyi-import-bazovykh-stantcii-v-rf-udalos-naladit (accessed May 29, 2023).

59 Marina Tyunyaeva (Bochkareva), "Правительство не отменяет ответственность за пиратский софт из недружественных стран" [The government does not abolish responsibility for pirated software from unfriendly countries], *Vedomosti*, March 11, 2022: https://www.vedomosti.ru/technology/articles/2022/03/11/913009-otvetstvennost-piratskii-soft (accessed May 17, 2023).

60 Ekaterina Kinyakina Anna Ustinova, "Пользователи иностранного ПО профинансируют льготные IT-кредиты" [Users of foreign software will finance preferential IT-credits], *Vedomosti*, May 17, 2023: https://www.vedomosti.ru/technology/articles/2023/05/17/975385-polzovateli-inostrannogo-po-profinansiruyut-lgotnie-it-krediti-rossiyanam?utm_campaign=newspaper_17_5_2023&utm_medium=email&utm_source=vedomosti (accessed May 17, 2023).

61 Interfax, "В РФ к концу марта предложат механизм использования зарубежного ПО без российских аналогов" [By the end of March the Russian Federation will propose a mechanism for the use of foreign software without Russian counterparts], February 28, 2023: https://www.interfax.ru/digital/889060 (accessed May 17, 2023).

vanced technology development that Russia so urgently needs has become less likely. It is difficult to assess the exact number of IT specialists who have left Russia since February 24, 2022, but various sources indicate an enormous loss of human capital. According to Maksut Shadayev, the Minister of Digital Development, Communications, and Mass Media of the Russian Federation, around 100,000 IT specialists have left Russia.[62] However, several independent estimations cite figures that are much higher – for example, up to a quarter of Russia's 1.7 million IT specialists.[63] The severe lack of middle- and senior-level IT personnel that has recently emerged on the Russian market is making it obvious that those who have left the country are predominantly highly qualified and experienced specialists.[64]

CONCLUSIONS

The export controls and IT-related sanctions that were introduced against Russia are working and represent an unprecedented response to its full-scale invasion of Ukraine. In a highly united and coordinated manner, Western countries have targeted the most critical components, entities, and research institutions involved in Russia's development of advanced technologies. Even if their assumed impacts took a different route, the measures have had a visible effect. Russia's government has had to revise its goals and plans for tech development. Most notably, Russia's telecommunications infrastructure is suffering, and the lack of high-end chips has affected companies in various industries, especially AI. Russia's measures to mitigate the harm caused by the restrictive measures are leading to more dependency on third countries, vulnerability, and information security risks.

Because Russia has always relied on Western technologies, the sanctions and restrictions are disrupting the base upon which its modernization was being built. In the past, when favorable conditions for domestic innovation and technological breakthroughs were missing, Russia's economy could always profit from technology developed in the West. A total switch to domestic analogues or technologies from third countries would imply a fundamental change that would take at least five to ten years to implement – with unforeseeable outcomes, if such a change is feasible at all. Consequently, one can only predict that Russia will dramatically fall behind leading industrial countries. Even if the sanctions were lifted immediately, it would take Russia's tech industry years to recover and catch up to competitive standards. Considering Russia's growing technological stagnation, Vladimir Putin's ambition to turn Russia into a technological power has failed, and his rhetoric in this regard is – more than ever – an empty promise. Especially because the tech sanctions are weakening Russia's economic and geopolitical standing and the country's development, its outlook is now much more precarious.

Yet the success of the introduced sanctions and export controls depends on their implementation. In particular, the United States has shown an unprecedented determination to use its power in the tech industry against Russia. The European Union has followed and joined these efforts. Nevertheless, the EU's implementation mechanisms are on a national level, meaning that unity and coordination are key. As Russia is preparing for a protracted war, the European Union must make unity and coordination among its member states its ongoing priority. If the EU wants to see the full effects of its restrictive measures, sanction evasion via third countries must also be stopped immediately.

Despite many public announcements to the contrary, there are still hundreds of Western companies operating in Russia. This is also true for the tech sector. Especially those tech companies that are involved in facilitating Russia's military power and surveillance capacities must be stopped and sanctioned immediately. At the same time, differentiation is needed. Several Western companies are providing internet connectivity and social media platforms that are crucial to keeping uncensored communication channels open for the Russian people. They provide the technical requirements and services for free information distribution, for example about the war. Those companies can prevent the regime from gaining the monopoly in the country's information space and fragmenting the global internet. Therefore, such companies should not only remain in Russia despite the pressures of Putin's regime, but also be spared Western sanctions.

62 AFP, "Moscow Says 100K IT Specialists Have Left Russia This Year," *The Moscow Times*, December 20, 2022: https://www.themoscowtimes.com/2022/12/20/moscow-says-100k-it-specialists-have-left-russia-this-year-a79754 (accessed May 17, 2023).

63 Eurasianet, "Россия: К Чему Приведёт Массовый Исход Айтишников?" [Russia: What Will the Mass Exodus of IT Workers Lead to?], October 31, 2022: https://russian.eurasianet.org/россия-к-чему-приведёт-массовый-исход-айтишников (accessed March 20, 2023).

64 Ibid.

In combination, the restrictive measures, the overall worsening of the economic and political situation in Russia, and the immediate risk of military mobilization have accelerated the brain drain of IT specialists. The urgent need for highly trained human capital will constrain Russia's technological goals more than ever. Further, because the restrictive measures also target universities and research centers, the education and training of young IT specialists has been substantially affected. Russia's scientific community is effectively excluded from relevant international collaborations and academic debates, which sets Russia even further back in global terms.

A clear beneficiary of Russia's current situation is China. The country has become crucial for Russia, especially in terms of evading export controls and providing chip imports, and it helps Russia maintain its economy and military. Mostly second- and third-tier Chinese manufacturers are digging into the Russian market and taking over the many customers left by Western companies. At the same time, China is keeping a safe distance. Leading Chinese tech company Huawei has stopped its exports to Russia out of fear of US sanctions. Also, there is no sign that Beijing will support Russia's development of emerging technologies. Several factors on both sides play into this.

One major factor for China's reluctance is its own dependence on critical components and equipment for advanced chipmaking from the West. As long as China is not self-sufficient in this area, its own AI development would be immediately threatened if sanctions were to be extended to Chinese advanced tech. Therefore, Beijing has no interest in becoming more involved with Russia. As for strategic technologies such as the processors used in its military-industrial complex, China is even less willing to help Russia. China has no reason to empower Russia to a level at which it could use advanced technology to compromise China's own information security. Moreover, Russia becoming a technologically strong and globally competitive neighbor is not in China's interest. Currently, China tends to see Russia as an opportunity: as an additional market on which there is hardly any international competition; as another source of human capital for its own research and development; and, most importantly, as a useful instrument in challenging the West and reshaping the global order on its own terms – without having to be directly involved.

On the Russian side, security concerns constrain the deepening of Sino-Russian collaboration on emerging tech. At first glance, these concerns relate to the development of Russia's mobile network, which requires the use of frequencies employed by its military. However, a closer look reveals that they stem from a justified, fundamental fear of being subsumed by China's predominance in the digital domain. Therefore, Russia currently allows only smaller, less advanced, and less relevant Chinese companies to provide it with technologies. Because they offer lower quality products and can only help maintain existing infrastructure, it is unlikely that they will foster any technological development and economic advantages for Russia.

Even though Russia is limiting itself by using such lesser Chinese technology, the risks for the West should not be underestimated. Combined Sino-Russian efforts – for example, in asymmetric cyber warfare – could pose a serious threat to the EU and its partners. It seems likely that China and Russia will join their efforts to exploit vulnerabilities related to the military and critical infrastructure and to engage in economic espionage in the West. Russia's experience in disinformation campaigns might be of use to China – and even enhanced by the powerful means of AI technology.

The international coalition must consider discrepancies between assumed impacts and real developments when implementing tech sanctions

At a time of increased technological competition, careful assessment of the impact made by the export controls and sanctions described here could provide

Western countries with a better understanding of the implication of such tools for foreign policy. The early results of the restrictive measures toward Russia show how they significantly limit an adversary's access to critical components and contribute to deficiencies in emerging technologies. If such knowledge could be combined with the experience gained by implementing a part of those restrictions toward China, it could help establish a broader framework and policy for regulating advanced technologies that, in turn, could prevent their spread in authoritarian countries. Therefore, the EU should strengthen its coordination with its partners and increase cooperation in such fora as the US-EU Trade and Technology Council (TTC).

While the broad and comprehensive set of export controls is an important step, the EU and its partners now need to focus on their implementation. Better monitoring and information-sharing should serve to rapidly identify and prosecute networks used to evade sanctions. International cooperation among governments, tech companies, investigative journalists, and the expert community is also key for uncovering and preventing shipments of controlled goods to Russia via third countries.

Moreover, the EU and its partners should assess the long-term consequences that Russia's technological backsliding will have on its economic development and social structure. When considering different scenarios for the outcome of Russia's war of aggression in Ukraine and its impact on Putin's regime, the EU should always include analysis of Russia's technological capabilities. Because freedom and democracy are already highly linked to technological development, and they will be even more so in the future.

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