ISSUE BRIEF

JULY 2024

Russia's Digital Tech Isolationism

Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology

JUSTIN SHERMAN

EXECUTIVE SUMMARY

Digital technology has long been a key component of the Russian government's power, and for years following the collapse of the Soviet Union there was significant technology entanglement between Russia, the West, and other areas of the world. That changed in the late 2000s and early 2010s with heightened paranoia within the Kremlin about regime security and foreign subversion—and Russia's 2022 full-scale invasion of Ukraine has taken this to new levels. Due to combinations of intense securitization, Western sanctions, foreign businesses exiting Russia, tech "brain drain," and other factors, digital technological isolationism is now both a reality and a desired goal for Moscow. This report examines the history of the modern Russian state's approach to digital technology, the internet, and connection and interdependence with the West and foreign countries. It then analyzes the Kremlin's late 2000s and early 2010s shift to a heavily securitized approach to the internet and its concerted push to develop domestic digital technology—both the successes and many failures. It then examines the 2022 Russian war on Ukraine, how the conflict and resulting events (such as sanctions and brain drain) have shifted Russia's approach to domestic technology and digital isolation, and where different digital technology segments, such as hardware and software, stand. The analysis concludes with five key takeaways for the US and its allies and partners, paired with recommendations:

1. Russia has even fewer incentives today to stop pursuing an isolationist and securitized approach to digital technology.

2. Russian companies have shown more success in building their own domestic software than domestic hardware.

3. The Russian cybersecurity sector will play an important role in Moscow's reaction to sanctions and its efforts to technologically isolate itself from the West.

4. Some Russian technology companies are already looking to the international market to expand their profit streams, including in internet and cybersecurity services.

5. Russia is becoming more digitally dependent on China.

The **Cyber Statecraft Initiative**, part of the ACTech programs, works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

TABLE OF CONTENTS

INTRODUCTION

Digital technology has long been a key component of the Russian government's power, from launching cyber operations to creating propaganda content. But in Russia, as in many countries, software and hardware have done far more than just support cyber and information operations: they have contributed to state economic modernization efforts, underpinned the government's growing surveillance of its own citizens, and enabled technological and intellectual connectivity between populations at home and abroad. For years, this technology drew from a diversity of international sources: Russia, China, Europe, the United States, Japan, and elsewhere. Conversely, many companies outside of Russia depended upon the labor and skills of Russian developers and engineers, many of whom provided remote services. Western technology such as the Microsoft Windows operating system was found all throughout Russia in the 2000s. But as the state became more paranoid about the internet as a threat to regime security, the Kremlin increasingly advocated for building domestic software and hardware and instituted policies to shift the government away from using Western digital technology. The government also introduced tax and other incentives for Russian tech developers to stay in Russia. A regime security approach came to dominate Russian policy.

Since the Putin regime launched its full-scale war on Ukraine in February 2022, this environment has been replaced with a new level of Russian techno-isolationism. The US, European allies, and other countries have imposed sanctions on a range of Russian digital technology companies and services. Countless global technology companies have terminated or severely curtailed their business activities in Russia, due to sanctions compliance, concerns over employee safety, support for Ukraine, signaling resolve to Western governments, restrictions from the Russian government, or a combination thereof. Around 100,000 Russian technologists (at least) fled the country by December 2022 to seek out economic opportunity and a less repressive political environment elsewhere, further accelerating Russia's "brain drain" problems.[1]

Technological isolationism is now both a reality and a desired goal for many in the Russian government and technology sector.

Simultaneously, the Russian government has accelerated its push to remove Western digital technology from the country and develop domestic software and hardware replacements that can be used in military and intelligence activities, bring money into Russia (at least in the state's hope), and serve as a means of expanding Russia's technology influence abroad. The Kremlin notably exempted Russian information technology workers from military conscription to fight in Ukraine, and it continues its frantic attempts to stem the departure of technology talent. Sanctions mitigation and evasion are now frequent topics of conversation in the Russian cyber community. All told, a greater degree of digital technological isolationism is now both a reality and a desired goal for many in the Russian government and technology sector.

This raises numerous questions for Western policymakers. As Russia's economy continues to shift during the war[2]—and sanc-

1 "About 100,000 IT specialists left Russia in 2022 – digital development minister," *Interfax*, December 20, 2022, https://interfax.com/newsroom/top-stories/86316/.

2 See, e.g., Emil Wannheden, *Russia's Wartime Economy — Neither Boom nor Bust* (Stockholm: Swedish Defense Research Agency, October 2023); FOI Memo 8236, https://www.foi.se/rest-api/report/FOI%20Memo%208236; "Russia Falls Into Recession," *The Moscow Times*, November 17, 2022, https://www.themoscowtimes.com/2022/11/16/russia-falls-into-recession-a79398.

tions continue to impose at least some costs on Russia's digital technology industry—the government, tech industry, and tech civil society in Russia are grappling with issues such as developing software alternatives to foreign app stores and operating systems, buying hardware from non-Western sources, illicitly acquiring hardware from Western sources, keeping tech talent in the country, fostering the next generation of cyber talent (including in support of the security services), and expanding Russia's tech market share abroad. For example, some Russian cybersecurity companies that support the Russian intelligence community are increasingly talking about selling their software overseas—in Latin America, in the Middle East, and elsewhere. Russia has also become more dependent on Chinese digital technology in the last two years.

But to quote historian Stephen Kotkin, "the Russian state can confound analysts who truck in binaries."[3] Despite these clear or emerging trends, the reality of Russia's digital tech ecosystem today is also complicated, messy, and in many ways uncertain. This report therefore presents five key takeaways from the analysis of this reality, paired below with implications for US policymakers and those in allied and partner countries. It focuses on digital technologies and companies—such as software, hardware, and Russian cybersecurity companies—rather than technology broadly, such as biotechnology and manufacturing technologies.

Key takeaways:

1. Russia has even fewer incentives (and even less room) today to stop pursuing an isolationist and securitized approach to digital technology—with impacts across international tech engagement, domestic policy, and human rights.

2. Russian companies have shown more success building their own domestic software than domestic hardware.

3. The Russian cybersecurity sector will play an important role in Moscow's reaction to growing sanctions and other restrictions as well as its efforts to technologically isolate itself from the West.

4. Some Russian technology companies are already looking to the international market to expand their profit streams, including in internet and cybersecurity services.

5. Russia is becoming more digitally dependent on China.

CREEPING SUSPICION: RUSSIAN DOMESTIC TECHNOLOGY FROM THE 1990S TO MID-2010S

Over the last three decades, Russia's technology sector has undergone a notable shift. In the 1990s and early 2000s, Russia's burgeoning internet services and technology sector used Western software and hardware without much question. Russian tech-focused universities collaborated with foreign institutions, and many Western companies, even in the cybersecurity sphere, struck up partnerships with rapidly expanding Russian businesses. Firms were also less dependent on China, and Russian tech companies had the freedom to operate abroad. Then, in the late 2000s and early 2010s, as high-level Kremlin officials became increasingly concerned about the internet as a regime security threat, and as those already concerned gained more power within the Putin regime, the Russian government made a concerted push to replace Western hardware and especially software. The resulting policies did not immediately rid Russia of foreign technology (and still have not done so). But domestic technology and restricted tech procurement became the name of the game—and in practice, there have been many bumps in the road.

Following the collapse of the Soviet Union, the Russian government was forced to contend with a confluence of challenges in its technology sector. There were many talented individuals in Russia with expertise in fields like computer science, physics, mathematics, and engineering.[4] Some moved out of the country to seek economic opportunities. Some turned to cybercrime, a far more lucrative profession amid an economy with limited jobs, widespread criminal enterprise, and insufficient laws.[5] Others yet founded companies. The security services, meanwhile, expanded their focus on internet surveillance and laid the foundation for the Kremlin's later, high-level concern about the internet as a regime security threat.

3 Stephen Kotkin, "Technology and Governance in Russia: Possibilities," Hoover Institution, October 3, 2018, https://www.hoover.org/research/technology-and-governance-russia-possibilities.

4 See, e.g., R. Adam Moody, "Reexamining Brain Drain from the Former Soviet Union," *The Nonproliferation Review* (Spring/Summer 1996): 92-97, https://www.nonproliferation.org/wp-content/uploads/npr/moody33.pdf; Andrei V. Korobkov and Zhanna A. Zaionchkovskaia, "Russian brain drain: Myths v. reality," *Communist and Post-Communist Studies* 45, no. 3-4 (September-December 2012): 327-341, https://www.sciencedirect.com/science/article/abs/pii/S0967067X1200058X; Ina Ganguli, "Scientific Brain Drain and Human Capital Formation After the End of the Soviet Union," European University Institute, 2013, https://cadmus.eui.eu/bitstream/handle/1814/27883/CARIM-East_RR-2013-26.pdf;jsessionid=AFA7EAF7E62CDE43D0032BA6F92B41F0?sequence=1.

5 Dmitri Alperovitch and Keith Mularski, "Fighting Russian Cybercrime Mobsters: Report from the Trenches," Black Hat, July 25-30, 2009, https://www.blackhat.com/presentations/bh-usa-09/ALPEROVITCH/BHUSA09-Alperovitch-RussCybercrime-PAPER.pdf, 2.

Notable Russian technology firms include Yandex, now a search and internet services giant, which was created in 1997[6] after its founders started building search programs for the Bible, the International Classifier of Patents, and more.[7] (It is worth noting that Yandex was even ahead of Google, which was founded in 1998).[8] Mail.ru, an internet service and now technology conglomerate in Russia (presently operating under the VK brand, now a Russian internet and social media conglomerate), was founded in 1998 as an email service provider for Russians.[9] Russian search engine *Rambler*, later bought by the Russian company Prof-Media (a media conglomerate and investment group) and then Russia's state-owned bank Sber, was founded around the same time and quickly took up market share as well.[10] Other examples of technology development and proliferation abound.

The Russian technology sector in the late 1990s and 2000s relied heavily on Western software and hardware. President Bill Clinton's administration modified US export control rules in 1999 to permit the sale of faster computers to Russia (and China).[11] Many of the large chips and electronics distributors in Russia in the 1990s and 2000s sold equipment from the likes of AMD (US-based), Intel (US), Motorola (US), Samsung (South Korea), Texas Instruments (US), Toshiba (Japan), and Philips (Netherlands).[12] Motorola (US), Nokia (Finland), and Samsung (South Korea) dominated Russia's 2000s mobile phone market.[13] The open-source Linux operating system was widely used in the region, and billions of dollars of Linux-related technologies were sold in Russia and the former Soviet republics in the early 2000s.[14] In early 2005, Microsoft made the Windows operating system available in Russia;[15] in October 2008, Apple launched iPhone sales with Russian retailers.[16] As more Russians used the internet at home,[17] the most-visited websites included Yandex, *Rambler*, and Mail.ru—which controlled the most market share—as well as non-Russian websites like Google and Yahoo, companies that quickly came to define the US tech sector.[18] Piracy of software, mainly Western software such as Microsoft Windows, was also rampant around this time, especially in the 1990s, with a 2001 industry report estimating that about 90% of Russia's software market at the time was pirated.[19]

Russian organizations also collaborated with foreign counterparts. After the Soviet Union's collapse in 1991, some Western businesses began to realize they could leverage the scientific and technical talent pools in Russia to outsource software development and other tasks.[20] In 1996, billionaire George Soros launched an effort to build and equip internet centers at Russian universities to link schools, hospitals, and other Russian organizations to the global internet.[21] In 2003, the University of Missouri launched a journalism education partnership with Moscow State University, which, relatively novel at the time,

6 "History of Yandex: 1997," Yandex.com, accessed November 16, 2022, https://yandex.com/company/history/1997.

7 "History of Yandex: 1990," Yandex.com, accessed November 16, 2022, https://yandex.com/company/history/1990.

8 "From the garage to the Googleplex," Google, accessed August 28, 2023, https://about.google/our-story/.

9 "Mail.Ru Group," Crunchbase.com, accessed November 16, 2022, https://www.crunchbase.com/organization/mail-ru.

10 « "Проф-Медиа" приобретает 54.8% *Rambler* Media », *Rambler*, October 31, 2006, https://web.archive.org/web/20061213022333/http://www.rambler.ru/db/press/msg.html?mid=9017070&s=260000269; « Сбербанк стал единственным владельцем *Rambler* », *RBC*, October 29, 2020, https://www.rbc.ru/business/29/10/2020/5f9af8339a79470b67836406.

11 Michael Lelyveld, "Russia: U.S. Takes Steps To Allow Super-Computer Sales," *Radio Free Europe/Radio Liberty*, July 9, 1999, https://www.rferl.org/a/1091683.html.

12 "Chip distributors in Russia," chipinfo.ru, June 30, 2002, http://www.chipinfo.ru/chipdir/dist/ru.htm.

13 Motorola had more trouble than the others, although due to patent disputes in Russia, not government opposition to Western devices. See: Guy Chazan, "Russia Puts Motorola on Hold," *The Wall Street Journal*, June 8, 2006, https://www.wsj.com/articles/SB114973190819574520.

14 Tom Adelstein, "Linux in Government: Outside the US, People Get It," *Linux Journal*, July 18, 2005, https://www.linuxjournal.com/article/8449.

15 "Windows XP Starter Edition Pilot Expands to Russia, India," Microsoft, September 27, 2004, https://news.microsoft.com/2004/09/27/windows-xp-starter-edition-pilot-expands-to-russia-india/.

16 "Russian retailers to start Apple iPhone sales Oct 3," *Reuters*, September 26, 2008, https://www.reuters.com/article/us-iphone-russia-retailersustech/russian-retailers-to-start-apple-iphone-sales-oct-3-idUSTRE48P3BX20080926.

17 "Half of Russian Internet users connect at home," *Sputnik International*, June 23, 2005, https://sputnikglobe.com/20050623/40750068.html.

18 See, e.g., "Most popular Russian sites – Yandex, *Rambler*, Mail.ru, Google," *ZDNet*, June 17, 2005, https://www.zdnet.com/article/most-popular-russian-sites-yandex-rambler-mail-ru-google/.

19 Elizabeth Williamson, "Software Piracy Rates in Eastern Europe Are Twice That of West, Report Says," *The Wall Street Journal*, June 25, 2001, https://www.wsj.com/articles/SB993403332336788539. See also: "A pirates' bazaar in Moscow offers treasured bootleg media," *Baltimore Sun*, December 11, 2002, https://www.baltimoresun.com/2002/12/11/a-pirates-bazaar-in-moscow-offers-treasured-bootleg-media/; Connie Neigel, "Piracy in Russia and China: A Different U.S. Reaction," *Law and Contemporary Problems* 63, no. 4 (2000): 179-199, https://www.jstor.org/stable/1192397?seq=7; Susan Tiefenbrun, "Piracy of Intellectual Property in China and the Former Soviet Union and its Effects upon International Trade: A Comparison," *Buffalo Law Review* 46, no. 1 (1998), https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=1460&context=buffalolawreview.

20 See, e.g., John Markoff, "Russian Computer Scientists Hired by American Company," *The New York Times*, March 3, 1992, https://www.nytimes.com/1992/03/03/business/russian-computer-scientists-hired-by-american-company.html; Maria Trombly, "Outsourcers Begin to Tap Russian Talent," *Computer World*, April 30, 2001, https://www.computerworld.com/article/2592184/outsourcers-begin-to-tap-russian-talent.html.

21 "Soros Plans to Finance Project to Develop Internet in Russia," *The New York Times*, January 15, 1996, https://www.nytimes.com/1996/01/15/business/soros-plans-to-finance-project-to-develop-internet-in-russia.html; Lee Hockstader, "U.S. Financier Gives Russia $100 Million for Internet Link," *The Washington Post*, March 19, 1996, https://www.washingtonpost.com/archive/politics/1996/03/16/us-financier-gives-russia-100-million-for-internet-link/0a0ce72b-d1bc-43ca-8d77-edf5f8388eb7/.

included using the internet to communicate between the two schools.[22] Cisco advised the Russian government on e-government strategy in the mid-2000s;[23] Russian cell provider MTS and British cell provider Vodafone signed a major agreement in October 2008, where MTS would receive "exclusive access to Vodafone's products and services" and in turn leverage the company's assistance in building third-generation (3G) cellular networks.[24] Russian programmers continued to grow the IT outsourcing industry in service of a variety of global businesses.[25] The list goes on. Some 1990s US sanctions issues and 2000s Putin anti-corruption raids notwithstanding,[26] the interconnectivity across borders was pronounced.

As the Russian technology sector grew into the internet age, so did the Russian security services. Boris Yeltsin signed a presidential decree in 1993 creating the Federal Agency of Government Communications and Information (FAPSI), the successor to the Committee for State Security (KGB)'s Eighth Chief Directorate, focused on signals interception at home and abroad.[27] Domestically, FAPSI ran SORM,[28] a surveillance system for intercepting telephone calls, emails, and other internet communications whose tactics and technology originated in a 1980s KGB research institute[29] (later expanded to its now-current SORM-3 version, which captures a range of telecommunications data). FAPSI also controlled licensing for information technology imports and exports, and, in 1994, it began coordinating telecommunication data-sharing between Russian security services and law enforcement agencies and those of countries in the Commonwealth of Independent States, or CIS (composed of Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan).[30] The agency answered directly to the Russian president.[31] Yeltsin intended to use FAPSI to, among other tasks, "support his battles with the political opposition at the top."[32]

In 1995, the Federal Security Service (FSB), the KGB's successor with some foreign and mostly domestic purview, took over the operation of the SORM system.[33] In 2000, the government began to let the tax police, the Ministry of the Interior (which controls the national police), and other institutions use SORM as well.[34] The FAPSI was dissolved in 2003, and its Third Directorate was mostly absorbed into the FSB in 2003; some of its functions were also transferred to the Federal Protection Service (FSO), such as providing strategic signals intelligence to Russian leadership and surveilling the internet.[35] The Federal Service for Technical Export and Control (FSTEK), a subcomponent of the Ministry of Defense, also played (and still plays) a role in licensing the export of dual-use technology items, military information security, and defense-focused control of Russian technology.[36]

Nonetheless, high-level Kremlin officials were not paying as much attention to the internet as a threat to regime security at this time, particularly compared to their counterparts in China. The security hardliners who were very much concerned and paying attention to this issue—such as intelligence heads pushing forward "information security," a sprawling concept of cyber-

22 "Partnership with Russia's Largest School of Journalism Announced," University of Missouri School of Journalism, February 10, 2003, https://journalism.missouri.edu/2003/02/partnership-with-russias-largest-school-of-journalism-announced/.

23 "Cisco in Europe," Cisco Systems, 2004, https://www.cisco.com/c/dam/global/fi_fi/assets/docs/solutions_europe.pdf.

24 "Vodafone, Russia's MTS sign services exchange deal," *Reuters*, October 30, 2008, https://www.reuters.com/article/vodafone-mts/vodafone-russias-mts-sign-services-exchange-deal-idINLT48607920081030.

25 F. Joseph Dresen, "The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification?" Wilson Center, April 17, 2006, https://www.wilsoncenter.org/publication/the-growth-russias-it-outsourcing-industry-the-beginning-russian-economic.

26 See, e.g., Jeff Gerth, "I.B.M. Unit Admits Illegal Sale of Computers to Russian Nuclear Lab," *The New York Times*, August 1, 1998, https://archive.nytimes.com/www.nytimes.com/library/tech/98/08/biztech/articles/01ibm.html; Dave Gradijan, "IBM's Moscow Office Raided in Fraud Investigation," *CSO Online*, December 8, 2006, https://www.csoonline.com/article/518844/data-protection-ibm-rsquo-s-moscow-office-raided-in-fraud-investigation.html.

27 "FAPSI Operations," Federation of the American Scientists, accessed November 21, 2020, https://fas.org/irp/world/russia/fapsi/ops.htm.

28 See, e.g., Gordon Bennett, *The Federal Security Service of the Russian Federation* (London: Conflict Studies Research Center, March 2000), https://www.files.ethz.ch/isn/96631/00_Mar_3.pdf.

29 Andrei Soldatov and Irina Borogan, "In Ex-Soviet States, Russian Spy Tech Still Watches You," *Wired*, December 21, 2012, https://www.wired.com/2012/12/russias-hand/.

30 Amy Knight, *Russia's New Security Services: An Assessment* (Washington, D.C.: Library of Congress Federal Research Division, October 1994), https://apps.dtic.mil/sti/tr/pdf/ADA299951.pdf, 38.

31 Ibid, 37.

32 Ibid, 5.

33 Julian Cooper, "The Internet as an Agent of Socio-Economic Modernization of the Russian Federation," in Markku Kangaspuro and Jeremy Smith, eds., *Modernization in Russia Since 1900* (Helsinki: Finnish Literature Society, 2006), 294.

34 Jen Tracy, "New KGB Takes Internet by SORM," *Mother Jones*, February 4, 2000, https://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm/.

35 Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: Public Affairs, 2010), 232; Roland Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm: Swedish Defense Research Agency, March 2010), FOI-R—2970—SE, https://foi.se/rest-api/report/FOI-R--2970--SE, 27-28.

36 Federal Service for Technical and Export Control, Government of Russia, accessed January 4, 2024, http://government.ru/en/department/96/.

security and information control[37]—did not yet have enough influence to drown out the "technocrats," elite technical experts in influential positions, and crystallize a highly securitized view of the internet.[38] The use of Western technology in Russia, the relatively uninhibited growth of the Russian technology sector from the 1990s into the 2000s, and technology partnerships between Russian and Western businesses and universities underscored this reality. As technology and security scholar Jackie Kerr incisively notes:

> *"Russia's moderate approach to the internet throughout this period was striking, given the extent to which it contrasted with the regime's demonstrated distrust of (and limited tolerance for) independent media, criticism, and social movements, as well as its growing paranoia about foreign and Western influence."* [39]

The Kremlin's "Internet Awakening"

Moscow's position on the internet began shifting in the late 2000s and early 2010s, catalyzed by a perception that Western technology was a means of foreign espionage, revolution-stoking, and influence-projection. The Kremlin's "internet awakening," as I would call it, was driven by a number of events, including the role of Georgian bloggers in the 2008 Russo-Georgian War, the use of social media in the 2010-2013 Arab Spring, online-organized protests against Putin's 2011 election rigging and 2012 return to the presidency, the 2013 Snowden leaks about US internet surveillance, and the 2014 social media-driven Euromaidan Revolution in Ukraine.[40] These events coincided with (and perhaps partly contributed to) the security hardliners in the Putin regime, already concerned about the internet years prior, gaining more power and influence—but now better equipped with the means to drive internet policy in the Russian political system.[41]

During this period, Moscow's cries of "color revolutions" and foreign interference were not simply propagandistic. The security services are rife with paranoia and conspiratorialism.[42] Key officials, including Putin himself, were trained in the KGB at a time in which the US and Soviet Union routinely interfered in foreign political systems. Some senior security figures also believe in pseudoscientific means of controlling human behavior through information, where "complex psychosocial phenomena," such as how populations of people think, are overlaid "with an innovative, mechanistic sense of order and control."[43] The influence of these security figures only grew in the 2000s as Putin restructured the government, consolidated power, reorganized the security services, and witnessed events such as the 2004-2005 Orange Revolution in Ukraine that provoked anger and paranoia.[44]

When Kremlin officials looked on television or their own streets in the late 2000s and early 2010s and saw people mobilizing against their governments—in part using American internet platforms—they did not see people with agency, acting of their own volition; they saw a foreign hand at work. While the fear of regime overthrow certainly predates the Russo-Georgian War and the Arab Spring, this was the first, major time that the Kremlin widely linked the internet to potential revolutionary peril.[45] Still today, many Russian foreign affairs commentators refer to the Arab Spring and similar, internet-involved events as "color revolutions."[46]

Alongside a crackdown on the internet in Russia,[47] the Russian government started talking more frequently in public about the

37 See, e.g., *Information Security Doctrine of the Russian Federation*, 2000, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf; Gavin Wilde and Justin Sherman, "No Water's Edge: Russia's Information War and Regime Security," Carnegie Endowment for International Peace, January 2023, https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.

38 Thanks to Carolina Vendil Pallin for additional discussion of this point.

39 Jaclyn A. Kerr, "Runet's Critical Juncture: The Ukraine War and the Battle for the Soul of the Web," *SAIS Review of International Affairs* 42, no. 2 (Summer/Fall 2022): 63-84, https://muse.jhu.edu/article/892250.

40 For a more detailed treatment of this evolving Kremlin thinking, see: Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Public Affairs, 2015); Justin Sherman, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior*, Atlantic Council, July 2021, 3-4, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/. For a more detailed analysis of the role of the Euromaidan in Moscow's internet threat perception and foreign election interference, see: Gavin Wilde and Justin Sherman, *Targeting Ukraine Through Washington: Russian Election Interference, Ukraine, and the 2024 US Election*, Atlantic Council, March 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/targeting-ukraine-through-washington/.

41 Thanks to Carolina Vendil Pallin for additional discussion of this point.

42 Martin Kragh, Erik Andermo, and Liliia Makashova, "Conspiracy theories in Russian security thinking," *Journal of Strategic Studies* (January 2020), https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1717954; Yulia Nikitina, "The 'Color Revolutions' and 'Arab Spring' in Russian Official Discourse," *Connections* 14, no. 1 (Winter 2014): 87-104, https://connections-qj.org/article/color-revolutions-and-arab-spring-russian-official-discourse.

43 Gavin Wilde, "In Russia's Information War, a New Field of Study Gains Traction," *New Lines Magazine*, September 14, 2022, https://newlinesmag.com/argument/in-russias-information-war-a-new-field-of-study-gains-traction/.

44 For a synopsis of some of the security service restructuring in the 2000s, see: Soldatov and Borogan, *The New Nobility*, 19-22.

45 For a thorough discussion of "color revolution" fears among Russian security experts, see: Graeme P. Herd, "Russia and the 'Orange Revolution': Response, Rhetoric, Reality?" *Connections* 4, no. 2 (Summer 2005): 15-28, https://connections-qj.org/article/russia-and-orange-revolution-response-rhetoric-reality

46 See, e.g., Elena Zinovieva and Bai Yajie, "Digital Sovereignty in Russia and China," Russian International Affairs Council, June 14, 2023, https://russiancouncil.ru/en/analytics-and-comments/analytics/digital-sovereignty-in-russia-and-china/.

47 See, e.g., Jackie Kerr, *The Russian Model of Internet Control and Its Significance* (Livermore: Lawrence Livermore National Lab, December 2018), https://www.osti.gov/biblio/1491981.

importance of domestic technology to replace foreign-made hardware and software, particularly from Western countries. Domestic tech was now the name of the game. Older comments buried in state documents—the 2000 Information Security Doctrine's call to "intensify development of the domestic production of information protection hardware and software, along with the methods to control their efficiency"[48]—were resurrected and given a stronger security bent.

> **"We must lessen our critical dependence on foreign technology."**
>
> *—Vladimir Putin, speech to Federal Assembly, December 2014*[49]

In a 2014 speech to the Federal Assembly, Putin iterated that "we must lessen our critical dependence on foreign technology" and that "import substitution programs must encourage the creation of a large group of industrial companies that can be competitive not only domestically but also on foreign markets."[50] The *2014 Military Doctrine* said the main internal military risks to Russia included activities aimed at "destabilizing [the] domestic political and social situation in the country" and "subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual, and patriotic traditions related to the defense of the Motherland."[51] Russia's 2015 *National Security Strategy* accuses the US and its allies of seeking to limit Russia's dominance in world affairs, including by exerting "political, economic, military, and informational pressure on it" and manipulating information and communication technologies.[52] The Kremlin's growing worries about the internet also stemmed from the extent to which Russian citizens' use of the internet (especially among young people) makes them less susceptible to state television propaganda.[53]

Western sanctions following Russia's illegal 2014 invasion and annexation of Crimea in Ukraine contributed to this trend as well.[54] At a meeting with defense industry executives in May 2014, for instance, Putin said that

> *"[Because of Western sanctions] we have new circumstances to address now—we need to replace imports. … [W]e need to do everything we can to have everything that our defense industry needs produced here on our own soil, so that we will not be dependent on anyone else for any of the new weapons systems we are delivering to our armed forces."*[55]

By that point in the year, the US had already issued a number of sanctions against Russian individuals and defense firms.[56] Notably, beginning in March 2014, the US Bureau of Industry and Security stopped issuing licenses for new exports of dual-use goods destined for Russia due to concern that they could be used in potential military applications.[57] These restrictions forced Moscow to rethink its digital technology acquisition and development plans.

The Russian state was not entirely unfamiliar with domestic technology initiatives. In 2007, for instance, the government stood up Rusnano, a state company, to produce and make Russia a leader in nanotechnology.[58] Despite the backing of several high-ranking officials and credentialed scientists, it failed to meet ambitious targets for 2011 due to a combination of limited technical talent, challenges with cultivating entrepreneurship, a lack of competence in business management, and, perhaps most importantly, a lack of domestic nanotechnology produc-

48 *Information Security Doctrine of the Russian Federation*, 2000, I.1.

49 "Presidential Address to the Federal Assembly," The Kremlin, December 4, 2014, http://en.kremlin.ru/events/president/news/47173.

50 Ibid.

51 *Military Doctrine of the Russian Federation*, 2014. II. 13, https://web.archive.org/web/20180501051233id_/ https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf.

52 *National Security Strategy of the Russian Federation*, 2015. II. 12. and II. 21, https://www.russiamatters.org/node/21421.

53 Denis Volkov, Stepan Goncharov, and Maria Snegovaya, "Russian Youth and Civic Engagement," Center for European Policy Analysis, September 29, 2020, https://cepa.org/comprehensive-reports/russian-youth-and-civic-engagement/.

54 Russian government policies and actions in response to Western sanctions of course went well beyond technology. See, e.g., Neil MacFarquhar and Alison Smale, "Russia Responds to Western Sanctions With Import Bans of Its Own," *The New York Times*, August 7, 2014, https://www.nytimes.com/2014/08/08/world/europe/russia-sanctions.html.

55 Clifford G. Gaddy and Barry W. Ickes, "Ukraine: A Prize Neither Russia Nor the West Can Afford to Win," Brookings Institution, May 22, 2014, https://www.brookings.edu/articles/ukraine-a-prize-neither-russia-nor-the-west-can-afford-to-win/.

56 See, e.g., "Treasury Sanctions Russian Officials, Members of the Russian Leadership's Inner Circle, and an Entity for Involvement in the Situation in Ukraine," US Department of the Treasury, March 20, 2014, https://home.treasury.gov/news/press-releases/jl23331; "FACT SHEET: Ukraine-Related Sanctions," The White House, March 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/03/17/fact-sheet-ukraine-related-sanctions; "Ukraine and Russia Sanctions," 2009-2017, US Department of State, accessed January 20, 2024, https://2009-2017.state.gov/e/eb/tfs/spi/ukrainerussia/.

57 Sam Skove, "U.S. Ceases Issuing Export Licenses on Some Goods Destined for Russia," *The Moscow Times*, March 27, 2014, https://www.themoscowtimes.com/2014/03/27/us-ceases-issuing-export-licenses-on-some-goods-destined-for-russia-a33399.

58 Quirin Schiermeier, "High hopes for Russia's nanotech firms: but an ambitious government initiative has been slow to incubate a domestic high-tech industry," *Nature* 461, no. 7267 (2009): 1036-1039.

tion capability, which the then-Ministry for Industry and Energy described in 2007 as at a critically low level.[59] Follow-on targets, such as companies mass-producing nanotechnologies beginning in 2013, were never met.[60] Since 2016, Rusnano has been on the edge of bankruptcy,[61] and corruption investigations have plagued its leadership.[62]

More robust policies to promote domestic technology development and foreign technology replacement soon followed, and Moscow's push for technological autarky picked up speed.

ACCELERATING THE PUSH: MOSCOW'S MID-2010S DOMESTIC TECHNOLOGY POLICIES

Russia's campaign to boost domestic technology and, where possible, replace Western technology with its own substitutes accelerated in the following years. These efforts ranged from domestic investments in high-tech sectors to creating a registry of domestic software, requiring the use of domestic microelectronics (such as in computer processing), and "isolating" Russia's internet.

Clarity in Russian Strategy

In Putin's 2014 address to the Federal Assembly, he launched the National Technology Initiative, an effort to stimulate the development of high-tech Russian industry sectors.[63] It focused on nine projects: what the government called AutoNet, AeroNet, EnergyNet, FinNet, FoodNet, HealthNet, MariNet, NeuroNet, and SafeNet.[64] (There are 68 approved NTI projects as of July 2023, but it is unclear how much these efforts have achieved; this is discussed further below.)[65] AutoNet, for example, is a public-private partnership to develop the Russian market for services, systems, and modern vehicles focused on logistics—what the initiative calls the "Internet of Transportation."[66] The goals of the overall initiative, as laid out in the subsequent 2016 strategy, included boosting the Russian economy and spending four percent of Russia's GDP on science and technology by 2035.[67] (This goal, as it turns out, was not achieved, as discussed further below.) All of this followed, or at least coincided with, a raft of new sanctions, mainly from the US and the EU, targeting Russia's financial, energy, and defense sectors, among other industries.[68]

Nevertheless, Moscow's efforts continued. The government passed a law to create a registry of domestic software products in 2015, which went into effect on January 1, 2016.[69] Its initial purpose was to establish a list of Russian software products that state organizations could use.[70] The registry contains products that either (i) are at least 50 percent Russian-owned, (ii) have less than thirty percent of revenue going to foreign beneficiaries, or (iii) are open-sourced with the relevant intellectual property owned by a Russian entity.[71] Around August 2016, about a year into the registry's launch, the executive director of Russia's Association of Software Developers said that "most customers already have an established IT infrastructure that uses foreign software" and that "it takes time to change procedures that have been established over so many years."[72] This effort occurred alongside a broader push in Russia to unify and digitize govern-

59 Fredrik Westerlund, *Russian Nanotechnology R&D: Thinking Big About Small Scale Science* (Stockholm: Swedish Defense Research Agency, June 2011), FOI-R—3197-SE. 37, 47-52, 140-142.

60 Anatoly Chubais, "RUSNANO: Fostering Innovations in Russia through Nanotechnology," USRBC's 18th Annual Meeting, San Francisco, October 20-21, 2010, 14, https://www.rusnano.com/upload/oldnews/Document/28506_3.pdf.

61 Alexander Etkind, *Russia Against Modernity* (Hoboken: Wiley, 2023), 34.

62 « Против бывшего партнера «Роснано» возбудили уголовное дело о хищении из компании $50 млн », *Vedomosti*, October 24, 2022, https://www.vedomosti.ru/economics/articles/2022/10/24/947149-protiv-bivshego-partnera-rosnano-vozbudili.

63 "Presidential Address to the Federal Assembly," The Kremlin, December 4, 2014, http://www.en.kremlin.ru/events/president/news/47173.

64 Dzhabrailov Shamkhal, "Russian Digital Economy: Artificial Intelligence R&D Support Strategy," presentation to the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), 2018, 2, https://www.unescap.org/sites/default/files/Session%203_%20Mr.%20Dzhabrailov%20Shamkhal_Russia.pdf.

65 « Реестр Проектов НТИ », NTI 2035, July 28, 2023, https://nti2035.ru/documents/docs/projects/Реестр%20проектов%20НТИ_28.07.2023.pdf.

66 "Autonet," AutoNet, accessed September 25, 2023, https://autonet-nti.ru/en/; "NTI Autonet," AutoNet, accessed September 25, 2023, https://autonet-nti.ru/en/autonet/.

67 "NTI National Technology Initiative," *TA Advisor*, December 21, 2021, https://tadviser.com/index.php/Company:National_Technology_Initiative_(NTI).

68 See, e.g., "A timeline of EU and US sanctions and Russia countersanctions," Cambridge University Press and Assessment, accessed January 20, 2024, https://static.cambridge.org/content/id/urn:cambridge.org:id:article:S1049096519001781/resource/name/S1049096519001781sup001.pdf.

69 « Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственныхи муниципальных нужд», *Digital Russia*, November 16, 2015, https://d-russia.ru/wp-content/uploads/2015/11/ac872y0wqioFnrRUeTnpGjEavWCfgEAo.pdf.

70 « Реестр российского ПО – инструкция для госзаказчиков », *Digital Russia*, February 26, 2016, https://d-russia.ru/reestr-rossijskogo-po-instrukciya-dlya-goszakazchikov.html; « Как попасть в реестр российского ПО: пошаговая инструкция », The Skolkovo Foundation , September 12, 2016, https://sk.ru/news/kak-popast-v-reestr-rossiyskogo-po-poshagovaya-instrukciya/.

71 Gijs Hillenius, "Russia scrapped open source plans to focus on self-reliance," Interoperable Europe, August 15, 2019, https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/unified-software-register.

72 Andrei Zdanevich, "Why do Russian officials still prefer to use Microsoft?" *Russia Beyond*, August 9, 2016, https://www.rbth.com/science_and_tech/2016/08/09/why-do-russian-officials-still-prefer-to-use-microsoft_619419.

ment procurement through contract registries, complaint databases, and a platform covering the entire procurement process from notice to audit and monitoring.[73]

By the end of 2016, Putin proposed launching a "large-scale, system-wide program to develop an economy of a new technological generation" and declared that "Russia's national and technological independence, in fact, our future depend on this."[74] The Russian government also expanded its payment card system that year, called Mir, which was launched in 2014 following sanctions against Russia for invading and annexing Crimea, Ukraine.[75]

Russian cybersecurity companies also began to face more challenges in the Western market. At the beginning of the decade, Russian cybersecurity giant Kaspersky Lab planned an initial public offering (IPO) in the US but then backed out of the plan in 2012, with its founder Eugene Kaspersky saying he wanted to keep control of the company's direction.[76] There were also some media reports emerging, which Kaspersky contested, discussing the company's relationships with Russian security organizations and its general need to align with the Kremlin's interests.[77] In 2018, the US Department of Defense, General Services Administration, and NASA banned the use of Kaspersky Lab hardware, software, and services on federal government systems.[78] Detailed, public revenue information for Kaspersky is not available—including about how the US ban impacted Kaspersky's revenue—but as of 2018, the company was making more than 85 percent of its revenue from outside Russia.[79] In June 2024, the Commerce Department banned the sale of Kaspersky antivirus and cybersecurity technologies in the US altogether.[80] Other Russian cyber firms, meanwhile, stayed under the public's radar in the 2010s. Positive Technologies, subsequently sanctioned by the US in 2021 and the EU in 2023 for supporting Russian intelligence operations, had offices in Massachusetts and London for most of the decade.[81]

"We all know who the chief administrator of the global internet is. And due to its volatility, we have to think about how to ensure our national security."

—Dmitry Peskov, Kremlin Press Secretary, November 28, 2017[82]

All of this coincided with the Russian government cracking down heavily on the internet, relative to its degrees of openness in the country in the 1990s and early 2000s. Notably, in August 2014, the Kremlin expanded the SORM-2 internet surveillance program beyond internet service providers (ISPs), requiring that all online service providers operating in Russia install the "black boxes" that enable the FSB to intercept traffic.[83] Putin that

73 Country case: Towards e-procurement in the Russia [sic] Federation," OECD, October 7, 2016, https://search.oecd.org/governance/procurement/toolbox/search/towards-e-procurement-russian-federation.pdf.

74 "Presidential Address to the Federal Assembly," The Kremlin, December 1, 2016, http://en.kremlin.ru/events/president/news/53379.

75 "Russia to issue 30mn national payment cards in 2016 – CBR head," *RT*, August 10, 2015, https://www.rt.com/business/312073-russia-national-payment-system/; "Russian Federation: Financial Infrastructure Technical Note: July 2016," The World Bank Group, July 2016, https://documents1.worldbank.org/curated/en/659541472539905263/pdf/108087-FSA-P157494-PUBLIC-Russia-FSAP-Update-II-TN-on-Financial-Infrastructure.pdf.

76 John E. Dunn, "Kaspersky Lab CEO Backs Out of IPO Plans," *CSO Online*, February 7, 2012, https://www.csoonline.com/article/534676/data-protection-kaspersky-lab-ceo-backs-out-of-ipo-plans.html; "Kaspersky to buy out U.S. investors, rules out IPO," *Reuters*, February 6, 2012, https://www.reuters.com/article/us-kaspersky/kaspersky-to-buy-out-u-s-investors-rules-out-ipo-idUSTRE81511Z20120206/.

77 See, e.g., Noah Shachtman, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals," *Wired*, July 23, 2012, https://www.wired.com/2012/07/ff-kaspersky/; Eugene Kaspersky, "What *Wired* Is Not Telling You – a Response to Noah Schathman's Article in *Wired* Magazine," Kaspersky, July 25, 2012, https://eugene.kaspersky.com/2012/07/25/what-wired-is-not-telling-you-a-response-to-noah-shachtmans-article-in-wired-magazine/; Carol Matlack, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *Bloomberg*, March 19, 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies; Corey Flintoff, "Kaspersky Lab: Based In Russia, Doing Cybersecurity in the West," *NPR*, August 10, 2015, https://www.npr.org/sections/alltechconsidered/2015/08/10/431247980/kaspersky-lab-a-cybersecurity-leader-with-ties-to-russian-govt.

78 Federal Acquisition Regulation; Use of Products and Services of Kaspersky Lab, 83 FR 28141, June 15, 2018, https://www.federalregister.gov/documents/2018/06/15/2018-12847/federal-acquisition-regulation-use-of-products-and-services-of-kaspersky-lab. See also the final rule: Federal Acquisition Regulation: Use of Products and Services of Kaspersky Lab, 84 FR 47861, September 10, 2019, https://www.federalregister.gov/documents/2019/09/10/2019-19360/federal-acquisition-regulation-use-of-products-and-services-of-kaspersky-lab.

79 Shane Harris, Gordon Lubold, and Paul Sonne, "How Kaspersky's Software Fell Under Suspicion of Spying on America," *The Wall Street Journal*, January 5, 2018, https://www.wsj.com/articles/how-kasperskys-software-fell-under-suspicion-of-spying-on-america-1515168888.

80 Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers," US Department of Commerce, June 20, 2024, https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers.

81 Justin Sherman, "Russia's Open-Source Code and Private-Sector Cybersecurity Ecosystem," NSI, February 22, 2023, https://nsiteam.com/russias-open-source-code-and-private-sector-cybersecurity-ecosystem/; "Treasury Sanctions Russia with Sweeping New Sanctions Authority," US Department of the Treasury, April 15, 2021, https://home.treasury.gov/news/press-releases/jy0127;, "Official Journal of the European Union," Volume 66, European Union, June 23, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2023:159I:FULL.

82 "Russia to launch 'independent internet' for BRICS nations – report," *RT*, November 28, 2017, https://www.rt.com/russia/411156-russia-to-launch-independent-internet/.

83 Sergey Kozlovsky, "Russia Just Doubled Its Internet Surveillance Program," *Global Voices*, August 15, 2014, https://globalvoices.org/2014/08/15/russia-sorm-medvedev-social-networks-internet/.

year infamously called the global internet a CIA project.[84] In a similar form, Kremlin press secretary Dmitry Peskov remarked in November 2017 that "We all know who the chief administrator of the global internet is. And due to its volatility, we have to think about how to ensure our national security."[85] The practice of widespread blocking of websites accelerated in March 2014 tied to the Russian government's illegal annexation of Crimea.[86]

Russian government strategic documents reflected this view. The 2016 *Information Security Doctrine of the Russian Federation* stated that the "intelligence services of certain states are increasingly using information and psychological tools with a view toward destabilizing the internal political and social situation in various regions around the world."[87] Russia's 2021 *National Security Strategy* for the first time specifically called out non-Russian technology companies, saying that they are "spreading unverified information."[88] A "distorted view of historical facts," it continued, "as well as events taking place in the Russian Federation and in the world, are imposed on internet users for political reasons."[89] Although the documents characteristically made these statements in passive voice, the actors supposedly threatening Russia were clear: the West, and especially the United States.

A particular Kremlin perspective on the internet was evolving, one in which the web was both a weapon to be used against Russia's enemies and a threat to regime security. It at once reflected the reality of a Putin regime using the internet to conduct cyber espionage, launch destructive cyberattacks, and spread mis- and disinformation while also monitoring online activity and dissent with intense paranoia. This view is championed by a president who, by at least one allegation, limits his own personal use of mobile phones and the internet.[90] This concern extended to all kinds of technologies, from operating systems to mobile app stores and social media platforms. More than cross-border connectivity, innovation, or anything else, Russian officials saw security risks.

Yet, Mixed Results in Practice

Despite all this rhetoric, practice once again diverged from policy. These gaps between domestic tech on paper and in reality were seen in surveillance, open-source software development, the development of a "Russian Silicon Valley," and microelectronics manufacturing, among other areas.

Many of Russia's domestic tech efforts in the 2010s were a mixed bag. The state has made little progress on its 2016 vision to spend 4% of the country's GDP on scientific R&D by 2035—an objective that was incredibly ambitious—if not unrealistic—for Russia. This lofty goal was part of Russia's broader, concerted push to promote domestic digital technology, and it was arguably driven in part by a belief that commercial funding and productization would necessarily rise to meet the state's interest in domestic digital technology. However, it did not. Data from the Organization for Economic Cooperation and Development (OECD) in Figure 1 shows that Russian spending on domestic R&D barely rose above one percent of GDP from the entire period of 2000-2020, even before the start of the 2022 Russian war on Ukraine and the Kremlin's even greater focus on defense and military technology.

84 Ewen MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup," *The Guardian*, April 24, 2014, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

85 "Russia to launch 'independent internet' for BRICS nations – report."

86 "Russia censors media by blocking websites and popular blog," *The Guardian*, March 14, 2014, https://www.theguardian.com/world/2014/mar/14/russia-bans-alexei-navalny-blog-opposition-news-websites.

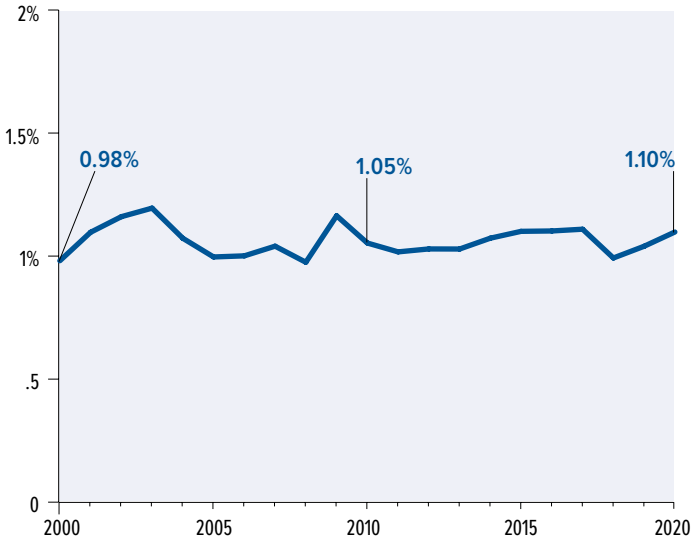
87 *Information Security Doctrine of the Russian Federation*, 2016, http://www.scrf.gov.ru/security/information/DIB_engl/.

88 *National Security Strategy of the Russian Federation*, 2021; "What You Need to Know About Russia's 2021 National Security Strategy," *Meduza*, July 5, 2021, https://meduza.io/en/feature/2021/07/05/what-you-need-to-know-about-russia-s-2021-national-security-strategy.

89 *National Security Strategy of the Russian Federation*, 2021; "What You Need to Know about Russia's 2021 National Security Strategy — Meduza."

90 Joshua Zitser, "Putin lives in an 'information vacuum' and never uses a cellphone or the internet, a Russian intelligence officer who defected says," *Business Insider*, April 4, 2023, https://www.businessinsider.com/vladimir-putin-never-uses-cellphone-internet-russian-defector-says-2023-4.

FIGURE 1: RUSSIAN GROSS DOMESTIC SPENDING ON R&D, AS A PERCENTAGE OF GDP (2000-2020)



Data Source: OECD[91]

Other challenges were exemplified in security and surveillance legislation. In 2018, Russia's parliament amended the Yarovaya law—a set of 2016 counterterrorism and security bills named after one of its authors, Irina Yarovaya, a member of the Russian parliament.[92] The amendment required telecommunications operators to store phone call recordings, text messages, internet traffic, and other information from users for up to six months, beginning in July 2018.[93] Yet it was quickly clear that many Russian telecommunications companies could not acquire the requisite equipment for this data collected domestically and instead would have to use Cisco (US), HP (US), and Huawei (China) technology to comply with the new data storage requirements.[94] On the one hand, the Russian security services further advanced their ability to access data and target dissent at home; on the other hand, the companies faced domestic tech shortfalls when implementing the data retention that caused further reliance on foreign technology companies. In May 2019, the state formalized a requirement for companies to use domestic data storage technology[95]—but the reality was still that many domestic offerings were insufficient to meet companies' needs.[96] Here also lay signals of a future problem for Russia: if the offerings in Russia were insufficient and the offerings in the West were not available, the country would likely be forced to turn to digital technologies from China.

Building domestic software products, on the other hand, may be one of the most successful areas of Russia's overall push. Google products remained popular in Russia in the 2000s and 2010s—YouTube is still one of the more widely used platforms—but Yandex controlled the majority of the search engine market domestically.[97] VK (then, VKontakte) was Russia's answer to Facebook; it is often dubbed "Russia's Facebook," in fact, because of the virtually identical interface. The platform was for years more popular than Facebook in Russia,[98] even as the Kremlin wrested the administration of the website away from its founder, Pavel Durov (who also founded Telegram), to clearly put it more clearly under state surveillance and control.[99] It is worth noting that this occurred by giving the ownership of VK to Mail.ru, the Russian tech conglomerate that already owned the social network Odnoklassniki and operated Russia's biggest email provider.[100] These and other domestic software products carved out market share that remained unconquered by US and non-Russian counterparts.

Not all products and services, of course, were as competitive. Rutube, developed in the mid-2000s as a YouTube alternative, switched in 2012 to a content aggregation model (after struggling to compete with the actual YouTube) and in December 2020

91 "Gross domestic spending on R&D," OECD, accessed January 3, 2024, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm.

92 "Russia: 'Big Brother' Law Harms Security, Rights," Human Rights Watch, July 12, 2016, https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

93 "The Yarovaya Law: One Year After," Digital Report Analytica, April 2017, 5, https://analytica.digital.report/wp-content/uploads/2017/07/The-Yarovaya-Law.pdf.

94 Maria Kolomychenko and Polina Nikolskaya, "Exclusive: Russia's telecoms security push hits snag – it needs foreign help," *Reuters*, July 5, 2018, https://www.reuters.com/article/us-russia-technology-dataprotection-excl/exclusive-russias-telecoms-security-push-hits-snag-it-needs-foreign-help-idUSKBN1JV12Y.

95 Постановление Правительства РФ от 28 мая 2019 г. N 673, Garant, May 28, 2019, https://base.garant.ru/72255540/.

96 This is reflected in many areas of Russia's domestic technology push, where there is widespread noncompliance with existing laws but the state continues to pass new ones anyway, far ahead of the tech reality and the compliance curve. See, e.g., Jon Porter, "Russia passes law forcing manufacturers to install Russian-made software," *The Verge*, December 3, 2019, https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphones-laptops.

97 « Что американцу монополия, то русскому... », *Kommersant*, October 24, 2020, https://www.kommersant.ru/doc/4547165.

98 Oleg Yegorov, "Facebook and Google's Russian rivals: Why are they winning?" *Russia Beyond*, February 12, 2019, https://www.rbth.com/science-and-tech/329970-russian-facebook-vk-russian-google-yandex.

99 See, e.g., Maria Kiselyova, "Usmanov tightens hold on Russian social net VKontakte as founder sells stake," *Reuters*, January 24, 2014, https://www.reuters.com/article/us-russia-vkontakte/usmanov-tightens-hold-on-russian-social-net-vkontakte-as-founder-sells-stake-idUSBREA0N1MA20140124; Kevin Rothrock, "Pavel Durov, Founder of Russia's #1 Social Network, Is Not Going to Prison (For Now)," *Global Voices*, June 8, 2013, https://globalvoices.org/2013/06/08/pavel-durov-founder-of-russias-1-social-network-is-not-going-to-prison-for-now/; Kevin Rothrock, "Pavel Durov, Russia's Zuckerberg, Fights for Control of His Creation," *Global Voices*, April 30, 2013, https://globalvoices.org/2013/04/30/pavel-durov-russias-zuckerberg-fights-for-control-of-his-creation/.

100 Mark Scott, "Mail.ru Takes Full Ownership of VKontakte, Russia's Largest Social Network," *The New York Times*, September 16, 2014, https://archive.nytimes.com/dealbook.nytimes.com/2014/09/16/mail-ru-takes-full-ownership-of-vkontakte-russias-largest-social-network/.

was purchased by the state-owned Gazprom Media to build out longer professional and amateur content for Russians.[101] As Gazprom then looked to develop its own TikTok-style product, Andrei Konyaev, of the digital science magazine *N+1*, commented that Rutube exemplified the challenge ahead: where a product already exists with millions of users in its base, Russians would not immediately go en masse to a new service.[102] Rutube has since expanded into areas such as streaming live mixed martial arts (MMA) fights.[103] For the time being, a more likely substitute appears to live with VK, which saw considerable growth in social media and content services in 2023.[104]

In 2015, Moscow reportedly looked to Jolla, a Finnish company, to provide a mobile operating system built specially for Russian use.[105] The chairman of the company, which develops the Linux-based Sailfish OS, said at the time that Russia's plan was to "have one code base but then to integrate local internet services and ecommerce services on the user interface."[106] Russian authorities chose Sailfish OS in 2016 as the mobile platform to develop further, yet, in 2021, the company began curtailing business in Russia and severed ties in 2022.[107] Now, Russian state-owned telecom Rostelecom is supposedly building an Aurora OS mobile operating system for Russia, the progress of which remains to be seen.[108]

At the same time, the Russian government also upped its interest in open-source software. This includes Astra Linux, a Linux-variant operating system developed by the Russian conglomerate Astra Linux Group (RusBITech-Astra LLC) in the late 2000s or early 2010s (depending on the source) based on the Debian version of Linux.[109] It has slowly become the Russian state's operating system of choice, now offering both a commercial version and one designed for handling secure information.[110]

In September 2018, the Ministry of Digital Development wrote that open-source software is safer to use than proprietary software in government settings because many applications from well-known developers have undocumented features that can be a security threat—but with open-source software, the state can access the source code and control this risk.[111] (This is, of course, not necessarily true but is an interesting perspective from the ministry nonetheless.) By September 2021, the state announced new plans to further support open-source software development, even though Microsoft Windows remained widely used in the country.[112] Based on images released by the Kremlin in December 2021, it even appeared that some of the computers in Putin's office still used Windows XP, which was originally released in 2001.[113]

Other domestic tech activities have fallen more on their face. The Skolkovo Innovation Center is a prime example. Established in 2010[114] to become, in aspiration, "Russia's Silicon Valley," the program had billions of dollars in Russian government funding and global partnerships with Siemens, IBM, Intel, Microsoft, and Cisco.[115] Upon its launch, then-President Dmitry Medvedev flew to Silicon Valley in California to meet with Apple's Steve Jobs, then-California Governor Arnold Schwarzenegger, and executives from Twitter, Google, and many companies—saying his

101 Ingrid Lunden, "Rutube, the YouTube of Russia, Links up with Facebok, Gets YouTube, Vimeo Vids in Aggregation Pivot," *TechCrunch*, June 29, 2012, https://techcrunch.com/2012/06/29/rutube-the-youtube-of-russia-links-up-with-facebook-gets-youtube-vimeo-videos/; « Россияне будут продолжать смотреть телевизор », *Kommersant*, December 23, 2020, https://www.kommersant.ru/doc/4625739.

102 « «Газпром-медиа» строит видеовертикаль », *Kommersant*, December 23, 2020, https://www.kommersant.ru/doc/4626686; "Andrey Konyaev," European Conference of Science Journalism, accessed September 18, 2023, http://www.ecsj2020.eu/speakers/andrey-konyaev/.

103 « Битва Титанов », *Kommersant*, December 23, 2021, https://www.kommersant.ru/doc/5142905.

104 Philipp Dietrich, "The Key Player in Russia's Cybersphere," German Council on Foreign Relations, September 2023), 10-11, https://dgap.org/system/files/article_pdfs/DGAP%20Analysis%20No.%204_September_20_2023_20pp.pdf.

105 Liam Tung, "The inside story of Russia's 'own mobile OS': It's not what you think," *ZDNet*, May 20, 2015, https://www.zdnet.com/article/the-inside-story-of-russias-own-mobile-os-its-not-what-you-think/.

106 Ibid.

107 "Sailfish OS licensing model," Sailfish, accessed January 4, 2024, https://sailfishos.org/cases/; Natasha Lomas, "Finland's Jolla, maker of Sailfish OS, is trying to cut ties with Russia," *TechCrunch*, March 1, 2022, https://techcrunch.com/2022/03/01/jolla-cut-ties-russia/.

108 Darnya Antoniuk, "Russia wants 2 million phones with home-grown Aurora OS for use by officials," *The Record*, June 2, 2023, https://therecord.media/russia-wants-phones-with-aurora-os.

109 "About," Astra Linux, accessed September 28, 2023, https://astralinux.ru/en/about; "Astra Linux," Wikipedia, April 17, 2023, https://en.wikipedia.org/wiki/Astra_Linux; "Astra Linux," Debian, accessed September 28, 2023, https://wiki.debian.org/Derivatives/Census/AstraLinux.

110 The secure version's source code is not publicly available online, even though Astra Linux is based on an open-source operating system.

111 « Свободное программное обеспечение в госорганах », Ministry of Digital Development, Communications and Mass Media of the Russian Federation, September 6, 2018, https://digital.gov.ru/ru/activity/directions/106/.

112 « Национальный репозиторий СПО предлагают наполнить софтом, созданным по госзаказу », Ministry of Digital Development, Communications and Mass Media of the Russian Federation, September 15, 2021, https://digital.gov.ru/ru/events/41270/.

113 Marc Bennetts, "Vladimir Putin 'still uses obsolete Windows XP' despite hacking risk," *The Guardian*, December 17, 2019, https://www.theguardian.com/world/2019/dec/17/vladimir-putin-still-uses-obsolete-windows-xp-despite-hacking-risk.

114 Russian Federal Law No. 244-FZ, September 28, 2010, https://www.wipo.int/wipolex/en/legislation/details/17945.

115 Elena Pakhomova, "City of the future: the trials and tribulations of Russia's Silicon Valley," New East Digital Archive, July 8, 2013, https://www.new-east-archive.org/articles/show/1177/future-city-trials-tribulations-russia-silicon-valley-skolkovo.

goal was to develop "full-fledged relations" and cooperation with companies.[116] Yet, the initial excitement quickly gave way to political fights and other problems. As journalist Alec Luhn wrote in 2013, "Skolkovo has in the past seemed like a typical pet project of Medvedev's: reform-minded, jumped up on economic modernization rhetoric, but producing little in the way of results."[117]

The state opened and later closed corruption investigations into some of the officials in charge, reportedly due to political fights against Medvedev and others in his faction[118]—a "tacit repudiation for Medvedev's dalliance with [the] West," as Gavin Wilde and I wrote in 2022.[119] By June 2015, many of the involved startups had emigrated from Russia and Skolkovo had shifted towards partnerships with Chinese companies.[120] Russian officials absurdly suggested this had nothing to do with Western sanctions post-Crimea annexation.[121] In 2022, Skolkovo was dealt another blow after MIT ended its partnership with Skolkovo, as many of the Western businesses involved with the center left the Russian market entirely.[122]

Domestic hardware manufacturing has been another significant pain point. The development of domestic computer chips and nanotechnology had been a state focal area since, at least, Rusnano's creation in 2007. Simultaneously, Russian spies continued to steal advanced microelectronics from the West for use in radar and surveillance systems, weapon guidance systems, and detonation triggers.[123] At a private Ministry of Digital Development meeting in December 2021, large buyers of Russian server equipment told state officials that they were dissatisfied with the cost, quality, and performance of domestic processors compared to foreign versions.[124] Russian chip manufacturers reportedly responded by pointing to Moscow's import substitution campaign and claimed that it was sufficient that the servers at least worked.[125] Of course, this is the bare minimum for an ostensibly functional technology product: that it functions.

This was not an isolated incident. The Moscow Center of SPARC Technologies (MCST) had spent years developing and manufacturing the Elbrus-8C processor,[126] designed to serve as a replacement for foreign components. It was an aspiration like many others in Russia's years-long push for greater technological independence. Yet when SberInfra—part of Russian bank Sber—tested the processor in January 2022, it found insufficient memory capacity, poor out-of-the-box software optimization, and other problems.[127] A Sber representative called the Elrbus-8C "very weak" compared to an Intel-made equivalent.[128]

> **"We're throwing rocks at the locomotive."**
>
> *—Alexei Venediktov, owner of Ekho Moskvy (Echo of Moscow) radio station, about Russia's then-legal ban on Telegram, April 13, 2018*[129]

Even on the surveillance front, the state's domestic technology capabilities were not at the level of sophistication the Kremlin desired. In 2018, the Russian government issued a legal ban on the encrypted messaging app Telegram, after Telegram said it could not provide encryption keys to the Russian government

116 Andrew Clark, "Dmitry Medvedev picks Silicon Valley's brains," *The Guardian*, June 23, 2010, https://www.theguardian.com/business/2010/jun/23/dmitry-medvedev-silicon-valley-visit.

117 Alec Luhn, "Not Just Oil and Oligarchs," *Slate*, December 9, 2013, https://slate.com/technology/2013/12/russias-innovation-city-skolkovo-plagued-by-doubts-but-it-continues-to-grow.html.

118 "Investigators uncover multi-million embezzlement in Skolkovo high-tech hub," *TASS*, February 13, 2013, https://tass.com/russianpress/689632; "Former Executive at Russian Innovations Hub Skolkovo Arrested in Absentia," *The Moscow Times*, July 27, 2015, https://www.themoscowtimes.com/2015/07/27/former-executive-at-russian-innovations-hub-skolkovo-arrested-in-absentia-a48554; Luhn, "Not Just Oil and Oligarchs."

119 Gavin Wilde and Justin Sherman, "Putin's internet plan: Dependency with a veneer of sovereignty," Brookings Institution, May 11, 2022, https://www.brookings.edu/articles/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/.

120 Mark Rice-Oxley, "Inside Skolkovo, Moscow's self-styled Silicon Valley," *The Guardian*, June 12, 2015, https://www.theguardian.com/cities/2015/jun/12/inside-skolkovo-moscows-self-styled-silicon-valley.

121 Ibid.

122 Phillip Martin, "MIT abandons Russian high-tech campus partnership in light of Ukraine invasion," *WGBH*, February 25, 2022, https://www.wgbh.org/news/local/2022-02-25/mit-abandons-russian-high-tech-campus-partnership-in-light-of-ukraine-invasion; Rebecca Fannin, "The Silicon Valley fallout from waging economic war against Russia," *CNBC*, March 17, 2022, https://www.cnbc.com/2022/03/17/the-silicon-valley-fallout-from-waging-economic-war-against-russia.html.

123 "Russian Agent and 10 Other Members of Procurement Network for Russian Military and Intelligence Operating in the U.S. and Russia Indicated in New York," US Federal Bureau of Investigation , October 3, 2012, https://archives.fbi.gov/archives/houston/press-releases/2012/russian-agent-and-10-other-members-of-procurement-network-for-russian-military-and-intelligence-operating-in-the-u.s.-and-russia-indicted-in-new-york.

124 « Суровый российский сервер », *Kommersant*, December 17, 2021, https://www.kommersant.ru/doc/5131374?from=main.

125 Ibid.

126 « Центральный процессор «Эльбрус-8С» (ТВГИ.431281.025) », MCST, accessed August 29, 2023, http://www.mcst.ru/elbrus-8c.

127 Anton Shilov, "Russian-Made Elbrus CPUs Fail Trials, 'A Completely Unacceptable Platform," *Tom's Hardware*, January 2, 2022, https://www.tomshardware.com/news/russias-biggest-bank-tests-elbrus-cpu-finds-it-unacceptable.

128 Ibid.

129 Andrew Roth, "Moscow court bans Telegram messaging app," *The Guardian*, April 13, 2018, https://www.theguardian.com/world/2018/apr/13/moscow-court-bans-telegram-messaging-app.

related to a 2017 terrorist attack in St. Petersburg.[130] Journalists, dissidents, and other Russians had also been using the app to share news and facilitate political conversations. For the next two years, the state tried and failed over and over again to block access to the app within Russia, due in part to Telegram's circumvention efforts such as using domain fronting, where traffic looks like it is going to one place but actually went to Telegram servers, as well as weaknesses in the state's internet censorship and deep packet inspection (DPI) filtering capabilities.[131] Even the Kremlin's press secretary, Dmitry Peskov, and other senior officials were still using the app while the ban was in effect.[132] Alexei Venediktov, the owner of Ekho Moskvy (the Echo of Moscow) radio station, quipped in April 2018 that "we're throwing rocks at the locomotive."[133]

In June 2020, the Russian government lifted the ban on Telegram, for a variety of likely reasons that include wasted time and resources to fail to block the app—as well as Pavel Durov's vague claim that Telegram had improved its ability to remove extremist content while also protecting privacy.[134] (There has also been reporting about Russian intelligence spying on Telegram chats in Ukraine.)[135] The state's filtering capabilities have improved somewhat but remained quite weak during this period.[136] Moscow's vision of a sovereign Russian internet, where internet regions could be isolated from the rest of the world at will, has similarly faced numerous challenges—and not just technical ones.[137] Of course, many other kinds of state surveillance, like the SORM internet monitoring system, remained in place and provided invasive data interception capabilities to the state security services alongside failed attempts at large-scale internet filtering.

And when all else fails, Moscow can wield offline violence and coercion, from detaining protestors to harassing dissidents to a notable example in September 2021: when Apple and Google refused to delete opposition leader Alexey Navalny's election app from their app stores, the Kremlin sent masked men with guns to Google's Moscow office, gave Apple and Google representatives lists of Russian employees that would be jailed, and even sent FSB agents to the home of Google's top executive in Russia and then followed her to a hotel—all to get the companies to comply.[138]

Meanwhile, Chinese telecommunications firm Huawei made significant inroads in Russia by playing into this Kremlin fear of Western technology. Newly signed partnerships with Russian telecom providers, meetings with state officials, and talk of broadly supporting Russia's "digital economy" all signified Huawei's greater access in a country increasingly worried about US and European subversion.[139] One Russian international affairs analyst importantly argued at the time that Chinese technology also came with espionage risks and that overdependence on non-Western technology was still a point of vulnerability.[140]

All told, the reasons behind these difficulties varied depending on the technology and policy in question. Domestic hardware development fell far short of stated goals, not least because of Russia's incredibly limited microelectronics manufacturing capacity. The Skolkovo Innovation Center was plagued by corruption, ineffective management, and political fights among Russian leadership. Efforts to isolate the internet were in many areas not given sufficient priority by the Kremlin and ran into companies simply dragging their feet, as with installing "black

130 "Russia to block Telegram app over encryption," *BBC*, April 13, 2018, https://www.bbc.com/news/technology-43752337.

131 Matt Burgess, "This is why Russia's attempts to block Telegram have failed," *Wired*, April 28, 2018, https://www.wired.co.uk/article/telegram-in-russia-blocked-web-app-ban-facebook-twitter-google.

132 "Kremlin Spokesman Still Uses Telegram Despite Ban," *The Moscow Times*, April 26, 2018, https://www.themoscowtimes.com/2018/04/26/kremlin-spokesman-still-uses-telegram-despite-ban-a61278; « Дворкович заявил, что у него работает Telegram, несмотря на блокировку », *TASS*, April 27, 2018, https://tass.ru/obschestvo/5160494. Cited in: Burgess, "This is why Russia's attempts to block Telegram have failed."

133 Roth, "Moscow court bans Telegram messaging app."

134 Justin Sherman, "What's behind Russia's decision to ditch its ban on Telegram?" Atlantic Council, June 26, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-behind-russias-decision-to-ditch-its-ban-on-telegram/.

135 Matt Tait, "Russia is spying on Telegram chats in occupied Ukrainian regions. Here's how," *Pwn All the Things*, December 2, 2022, https://www.pwnallthethings.com/p/russia-is-spying-on-telegram-chats.

136 See, e.g., Diwen Xue et al., *TSPU: Russia's Decentralized Censorship System* (Ann Arbor: Censored Planet, November 2022), https://censoredplanet.org/tspu.

137 Justin Sherman, *Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior*, Atlantic Council, July 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.

138 Max Seddon and Madhumita Murgia, "Apple and Google drop Navalny app after Kremlin piles on pressure," *Financial Times*, September 17, 2021, https://www.ft.com/content/faaada81-73d6-428c-8d74-88d273adbad3; Greg Miller and Joseph Menn, "Putin's prewar moves against U.S. tech giants laid groundwork for crackdown on free expression," *The Washington Post*, March 12, 2022, https://www.washingtonpost.com/world/2022/03/12/russia-putin-google-apple-navalny/.

139 Justin Sherman, "Huawei's push in Russia exploits Kremlin fears of Western technology," Atlantic Council, November 18, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/huaweis-push-in-russia-exploits-kremlin-fears-of-western-technology/.

140 Danil Bochkov, "China's Bid to Conquer Russia's 5G Market Should Worry the Kremlin," *The Diplomat*, October 14, 2020, https://thediplomat.com/2020/10/chinas-bid-to-conquer-russias-5g-market-should-worry-the-kremlin/.

boxes" on internet networks.[141] More broadly, as Russian international relations professor Tatiana Romanova noted in March 2015—a year after the Putin regime's invasion and annexation of Crimea, Ukraine—"import substitution requires huge investment at a time when resources are scarce."[142]

The Russian government is not the only actor influencing these dynamics. Different parts of Russian industry had their own mixed motives in dealing with the realities of sanctions compliance following the invasion of Crimea, trying to remain competitive in the global market, and pushing for self-serving domestic tech policies, among others. The US government was also concerned about how Russia-US tech engagement in the 2010s could enable Russian investors and others to steal American tech and trade secrets.[143] Given this paper's focus, though, the discussion of Russia's domestic tech push is meant to highlight just how Western sanctions in 2014, the Kremlin's "internet awakening" and growing paranoia about foreign technology, and other factors catalyzed a push for Russia's relative technological independence.

Headed into 2022, the march towards domestic technology—across state software procurement, moves to expel Microsoft Windows, and more—continued apace.

THE 2022 RUSSIAN WAR ON UKRAINE AND EVOLVING TECHNO-ISOLATIONISM

Since its full-scale invasion of Ukraine began in February 2022, Russia's relative technological isolationism has rapidly accelerated. Combinations of escalating "brain drain" and a frantic state push to retain domestic tech talent, Western tech companies exiting Russia, some forced and some self-serving private-sector excitement at domestic tech efforts, and more success with software than hardware have produced a landscape in which the Russian tech sector under Vladimir Putin's rule is forced to contend with more isolation than ever before. Russia also faces persistent roadblocks to investing greater resources in domestic technology development and has become far more dependent on digital technology from China since the war's inception.

Brain drain has been a problem in Russia for decades, but the 2022 Russian war on Ukraine elevated Russia's tech brain drain to new heights. In the months after the war began, numerous Russian programmers and other technically talented individuals left the country.[144] The Russian Association for Electronic Communications said that 50,000-70,000 IT specialists left in February and March 2022 alone.[145] Departures only grew in the ensuing period. Russia's Ministry of Digital Development reportedly estimated in December 2022 that approximately 100,000 IT workers had left Russia since February 2022, which the Ministry equated to 10 percent of Russia's entire technology workforce.[146] Former employees of Yandex, the Russian internet giant, "estimate that as many as a third left the country in just the first two months after the invasion," according to *MIT Technology Review*, although many still work remotely.[147] One study examined the listed online locations of active Russian developers, finding that between February 2021 and November 2022 about 11 percent of these developers had changed locations to a new country.[148]

This discourse on brain drain has also permeated the Russian tech community. Notably, Lev Gershenzon, the former head of Yandex News, called in March 2022 for his former colleagues to quit working at Yandex:

> *"The fact that a significant part of the Russian population may believe there is no war is the basis and driving force of this war... Today, Yandex is a key element in hiding information about war. Every day and hour of such 'news' costs*

141 Russian ISPs have had issues going back years with the state's insistence that they not only install black boxes but that they pay for the equipment, its installation, and its maintenance. See, e.g., Andrei Soldatov and Irina Borogan, "Inside the Red Web: Russia's back door onto the internet – extract," *The Guardian*, September 8, 2015, https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

142 Tatiana Romanova, "The Impact of Sanctions on Russia's Domestic and Foreign Policy," Chatham House, March 2015, 3, https://www.chathamhouse.org/sites/default/files/field/field_document/2015-03-24%20-%20The%20Impact%20of%20Sanctions%20-%20Event%20SummaryLP%20edited%20-JAKE.pdf.

143 Carl Schreck, "FBI Wary of Possible Russian Spies Lurking in U.S. Tech Sector," *Radio Free Europe/Radio Liberty*, May 17, 2014, https://www.rferl.org/a/fbi-wary-of-possible-russian-spies-in-lurking-in-us-tech-sector/25388490.html.

144 See, e.g., Cade Metz and Adam Satariano, "Russian Tech Industry Faces 'Brain Drain' as Workers Flee," *The New York Times*, April 13, 2022, https://www.nytimes.com/2022/04/13/technology/russia-tech-workers.html.

145 « ИТ-специалисты десятками тысяч уезжают из России », *C News*, March 22, 2022, https://www.cnews.ru/news/top/2022-03-22_poslableniya_ne_pomogayut.

146 "About 100,000 IT specialists left Russia in 2022 – digital development minister," *Interfax*, December 20, 2022, https://interfax.com/newsroom/top-stories/86316/.

147 Masha Borak, "How Russia killed its tech industry," *MIT Technology Review*, April 4, 2023, https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/.

148 Johannes Wachs, "Digital traces of brain drain: developers during the Russian invasion of Ukraine," *EPJ Data Science* 12, no. 14 (2023), https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-023-00389-3.

human lives. And you, my former colleagues, are also responsible for this."[149]

These reports collectively point to a staggering number of Russian residents who have left the country since February 2022 and brought their technological skills with them. And even if some of those individuals living outside of Russia work remotely for Russian companies, that still poses a challenge for Russia's tech sector: they may be unable to return to Russia, and once located in some foreign countries, technically talented Russians may have opportunities to make far more money by working for non-Russian companies than they had when living and working in the Russian market. These incentives are not new to the wartime period, but the starkness of the choices and the inability of many individuals to return to Russia have been heightened greatly since February 2022. This is not to say, of course, that there are no difficulties on the other side of this equation—including non-Russian companies hesitating to hire IT professionals who have recently left Russia.

Moscow has semi-frantically attempted to stem the tide. It upped tax incentives in March 2022 for qualified IT experts to remain in the country[150] and exempted some IT workers in September 2022 (along with some bankers and other professionals) from conscription into the military.[151] This followed tech companies in Russia, as well as Russia's Association of Software Developers, telling the Ministry of Digital Development that a widespread deployment of tech workers in combat would seriously harm the country, including by undermining support for the military and for "critical information infrastructure" facilities (as they are called in Russian law).[152]

In March 2023, the state announced that foreign software engineers could sign contracts with approved Russian tech companies without needing work permits.[153] Russian international affairs commentator Ifan Timofeev—also the program director for the well-known Valdai Discussion Club, which Putin frequents[154]—wrote in May 2023 that one of Russia's "biggest vulnerabilities is its industrial and human potential," citing the 2022 brain drain acceleration as a factor.[155] This feeling is clear among Russian members of parliament, some of whom were discussing the need for a law in December 2022 to prevent Russians who left the country from remotely working for many public- and private-sector organizations altogether.[156] This law did not materialize, though some Russian organizations like banks Sber and Tinkoff have restricted their employees' ability to work remotely from outside Russia.[157]

This outflow of technical talent from the country has merged with a broader exit of companies from the Russian market and persistent domestic technology challenges. Many non-Russian businesses have shuttered their operations in Russia and/or left the market entirely since February 2022. Their motivations for doing so include combinations of sanctions compliance, concerns over employee safety, support for Ukraine, signaling resolve to Western governments, and restrictions from the Russian government, among others. Western sanctions, for instance, have hit semiconductors, unmanned aerial vehicles (UAVs), and

149 Katie Canales, "The ex-news director of Russia's largest search engine urged his former colleagues to quit, accusing the company of censoring Russia's invasion into Ukraine," *Business Insider*, March 1, 2022, https://www.businessinsider.com/yandex-russia-former-news-director-urges-colleagues-quit-ukraine-invastion-2022-3.

150 "Russia announces new tax support measures for IT companies," CMS Law-Now, August 3, 2022, https://cms-lawnow.com/en/ealerts/2022/03/russia-announces-new-tax-support-measures-for-it-companies.

151 "Russia announces exemptions from Ukraine war mobilization," *Al Jazeera*, September 23, 2022, https://www.aljazeera.com/news/2022/9/23/russia-excludes-some-professionals-from-mobilisation; "Ukrainians Express Fear and Defiance as Staged Voting Begins," *The New York Times*, September 23, 2022, https://www.nytimes.com/live/2022/09/23/world/russia-ukraine-putin-news#russia-says-it-will-exempt-some-white-collar-workers-from-call-up-after-businesses-warn-of-repercussions.

152 « Авиация настраивает систему бронирования », *Kommersant*, September 23, 2022, https://www.kommersant.ru/doc/5572535; « IT-компании попросили Минцифры предоставить айтишникам отсрочку от мобилизации », *Forbes Russia*, September 22, 2022, https://www.forbes.ru/tekhnologii/477855-it-kompanii-poprosili-mincifry-predostavit-ajtisnikam-otsrocku-ot-mobilizacii.

153 "Russia Turns to Foreign IT Workers After Wartime Brain Drain," *The Moscow Times*, March 15, 2023, https://www.themoscowtimes.com/2023/03/15/russia-turns-to-foreign-it-workers-after-wartime-brain-drain-a80493.

154 See, e.g., "Vladimir Putin Meets with Members of the Valdai Discussion Club," Valdai Discussion Club, October 27, 2022, https://valdaiclub.com/events/posts/articles/vladimir-putin-meets-with-members-of-the-valdai-club/; Fiona Hill, "Dinner with Putin: Musings on the Politics of Modernization in Russia," Brookings Institution, October 8, 2010, https://www.brookings.edu/articles/dinner-with-putin-musings-on-the-politics-of-modernization-in-russia/.

155 Ivan Timofeev, "Ending Western domination is key to the emerging world order. Here's what needs to be done to achieve it," *RT*, May 30, 2023, https://www.rt.com/russia/576856-end-west-domination-world-order/.

156 « Б госдуму внесут закон о запрете удалённой работы из—за границы », *Verstka*, December 14, 2022, https://verstka.media/udalennuyu-rabotu-zapretyat?tg_rhash=86cf5f61f61288.

157 Mary Ilyushina, "Russia eyes pressure tactics to lure fleeing tech workers home," *The Washington Post*, March 8, 2023, https://www.washingtonpost.com/world/2023/03/08/russia-employers-intimidation-workers-war/#; "Russia goes after remote workers with tighter income tax draft law," *Reuters*, May 18, 2023, https://www.reuters.com/world/europe/russia-goes-after-remote-workers-with-tighter-income-tax-draft-law-2023-05-18/; "Key Russian bank limits remote work from abroad — RBK," *RT*, November 29, 2023, https://www.rt.com/business/588130-tinkoff-limits-remote-work-abroad/.

many other kinds of technologies;[158] companies providing information services to Russians, such as Google and Twitter (now X), are still active in the country.

Some businesses, like McDonald's, sold their in-country infrastructure to new Russian owners after they left.[159] The Russian government cracked down on other businesses that remained, such as officially designating Meta—the parent company of Facebook, WhatsApp, and Instagram—as an "extremist" organization.[160] This is at once propagandistic (by essentially labeling Facebook as a terrorist organization), sincere (in that the Kremlin genuinely believes Western tech platforms are operating at the behest of the US government),[161] and intended to enable further crackdowns (given that many repressive laws in Russia are oriented around the term "extremism").[162] All told, the historical engagements between Russian and Western businesses and universities in the technology sphere have given way to even more severed ties.

These Western sanctions and business departures have forced the Russian government, as well as Russian industry and civil society, to contend with tech replacement and acquisition problems more urgently than ever before. Russia's pre-February 2022 starting point was already worrisome for the Kremlin: a Bank of Finland analysis published in March 2022 found that Russia's industrial production shares of "medium- and high-technology sectors such as machinery [and] equipment have declined slightly over the past decade," with the exception of the pharmaceutical industry.[163] In some ways, Russia's tech dependence had also been shifting towards China: between 2013-2018, the study found, the percentage of Russian tech imports from the EU declined, while "China's share for technology sectors has grown visibly."[164] At a meeting in 2023 with European defense and intelligence analysts, one expert described this dynamic as Russia losing its strategic ability to counterbalance between tech dependence on the US and China. Now, Moscow is largely stuck with the latter.[165]

In the hardware sphere, Russia has struggled even more since than it did prior to the war. A key factor in this decline is that the state does not have a robust microelectronics capability. In May 2022, Alexander Kuleshov, a mathematician and technologist who took over the Skolkovo Innovation Center in 2021,[166] called Russia's supply of tech equipment a "disaster."[167] Equipment such as supercomputer boards break down frequently, he said, and the manufacturers of some equipment have terminated repair, maintenance, and other warranties.[168] News reports indicate that Russian intelligence organizations have evaded sanctions to purchase chips from third countries, and Russian forces have resorted in some cases to stripping down refrigerators and other appliances to use their chips in military gear.[169]

The aforementioned Elbrus processor—which the Russian state hoped could replace processors made by Intel and other US firms—was originally manufactured by TSMC in Taiwan.[170] After the 2022 Russian war on Ukraine began, TSMC stopped working with Russian companies, and the MCST that designs Elbrus had to pivot to the Mikron Group, a microelectronics company

158 "With Over 300 Sanctions, U.S. Targets Russia's Circumvention and Evasion, Military-Industrial Supply Chains, and Future Energy Revenues," US Department of the Treasury May 19, 2023, https://home.treasury.gov/news/press-releases/jy1494; "The United States Imposes Sanctions on Russian Entities Involved in UAV Deal with Iran," US Department of State, December 9, 2022, https://www.state.gov/the-united-states-imposes-sanctions-on-russian-entities-involved-in-uav-deal-with-iran/.

159 "McDonald's To Exit from Russia," McDonald's, May 16, 2022, https://corporate.mcdonalds.com/corpmcd/our-stories/article/mcd-exit-russia.html; Amelia Lucas, "McDonald's to sell Russian business to existing Siberian licensee," *CNBC*, May 19, 2022, https://www.cnbc.com/2022/05/19/mcdonalds-to-sell-russian-business-to-existing-siberian-licensee.html.

160 "Russia confirms Meta's designation as extremist," *BBC*, October 11, 2022, https://www.bbc.com/news/technology-63218095.

161 Justin Sherman, "Russia Signals a New Era in Its War on Western Internet Platforms," *Slate*, March 8, 2022, https://slate.com/technology/2022/03/russia-roskomnadzor-youtube-information-warfare.html.

162 See, e.g., The Structure of Russian Anti-Extremism Legislation," SOVA Center for Information and Analysis, November 2010, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/201/201011/20101129_3_10sova_en.pdf.

163 Heli Simola, *Made in Russia? Assessing Russia's Potential for Import Substitution* (Helsinki: Bank of Finland Institute for Emerging Economies, March 2022), 5, https://www.econstor.eu/handle/10419/253652.

164 Ibid., 14-15.

165 Author's conversation with European defense and intelligence analysts, August 2023.

166 "Alexander Kuleshov," Skoltech, January 3, 2021, https://www.skoltech.ru/en/team/alexander-kuleshov/.

167 « Тотального бегства иностранцев не наблюдаем, хотя отдельные обидные потери есть », *Kommersant*, May 22, 2022, https://www.kommersant.ru/doc/5357614.

168 Ibid.

169 "Special report: How U.S.-made chips are flowing into Russia," *Nikkei*, April 12, 2023, https://asia.nikkei.com/Business/Tech/Semiconductors/Special-report-How-U.S.-made-chips-are-flowing-into-Russia; "Web of Secret Chip Deals Allegedly Help US Tech Flow to Russia," *Bloomberg*, March 15, 2023, https://www.bloomberg.com/news/features/2023-03-15/secret-chip-deals-allegedly-help-us-technology-flow-to-russia-despite-sanctions#xj4y7vzkg; Zoya Sheftalovich and Laurens Cerulus, "The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke," *Politico Europe*, September 5, 2022, https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/.

170 "Elbrus processors developer preparing to transfer production to Zelenograd's Mikron from Taiwan – media," *Interfax*, May 30, 2022, https://interfax.com/newsroom/top-stories/79684/.

in Russia.[171] This is hardly a one-to-one replacement: TSMC is a global leader in semiconductor manufacturing, and Mikron Group (JSC Mikron), by some reports, cannot even meet the requirements to produce chips used in mobile phones, computers, and other devices.[172] JSC Mikron has also had some manufacturing infrastructure, at least historically, in China.[173] The only other major microelectronics company in Russia, Baikal Electronics—which makes ARM-based processors—also relied on TSMC to do most of its manufacturing, a partnership that is now terminated.[174] Other smaller Russian manufacturers have struggled in recent years with debt, and since sanctions during the war, "Russian chip-design firms have lost access to most foreign contract manufacturing."[175] Sources in the electronic manufacturing sector told the newspaper *Vedomosti* in March 2024 that over half of the processors made by Baikal Electronics are defective.[176]

Software is a more complete story than hardware. Russia's cybersecurity sector has many competitive companies, like Kaspersky and Positive Technologies; even with US and EU sanctions,[177] Positive Technologies has seen double-digit revenue growth in 2023 and is positioned for additional international growth in 2024.[178] The Astra Linux operating system has also grown in usage in recent months.[179] In May 2022, Russia's Ministry of Digital Development announced plans to take Russia's domestic software registry, which then had over 13,000 products, and turn it into a "full-fledged marketplace" for acquiring software (users located outside of Russia currently appear blocked from accessing the registry).[180] Some companies are also pushing the state to reduce the competitiveness of foreign products in Russia: in May 2022, for example, the Domestic Software Association, which represents over 220 tech companies, told the Ministry of Digital Development that it should not simplify the process for joining the domestic software registry because "the simplification may lead to [the] emergence of foreign software clones."[181] In short, while the state is rolling out many policies at once, it is reductive and inaccurate to treat Russia's tech ecosystem as a highly coordinated, top-down system in which companies and other stakeholders have no agency or influence.

For some Russian internet companies attempting to show distance from the state, such as Yandex—which sold off its news assets to VK in September 2022, as the Kremlin cranked up penalties for companies not bowing to its propaganda directives and wishes[182]—the major source of growth may be out of Russia. Yandex engaged in months of conversations, discussed more below, about restructuring the company to separate its publicly listed Dutch holding company from the Russian side of the business.[183] For years, the company has maintained business operations on other continents, including Europe. The Q3 2023 results from Yandex's public Dutch holding company showed quarterly revenue up 54% from the year prior.[184] An internet giant born in Russia in the 1990s may now be able to keep its growth—but, ironically, by cutting off its Russian arm. And as

171 "Elbrus Processors Developer Preparing to Transfer Production to Zelenograd's Mikron from Taiwan - Media."

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

173 "Silicon Trust welcomes JSC MIKRON as new partner," Silicon Trust, April 27, 2014, https://silicontrust.org/2014/04/27/silicon-trust-welcomes-jsc-mikron-as-new-partner/.

174 Pavel Urusov, "Vital Microchip Sanctions Will Hit Russian Computing Power Hard," Carnegie Endowment for International Peace, July 25, 2023, https://carnegieendowment.org/politika/90250.

175 Chris Miller, "The Impact of Semiconductor Sanctions on Russia," American Enterprise Institute, April 2024, 1-3, https://www.aei.org/research-products/report/the-impact-of-semiconductor-sanctions-on-russia/.

176 "Half the processors made by Russian computer chipmaker Baikal electronics are reportedly defective," *Meduza*, March 27, 2024, https://meduza.io/en/news/2024/03/27/half-the-processors-made-by-russian-computer-chipmaker-baikal-electronics-are-reportedly-defective; « Разработчик процессоров Baikal локализует один из этапов производства », *Vedomosti*, March 26, 2024, https://www.vedomosti.ru/technology/articles/2024/03/26/1027924-razrabotchik-protsessorov-baikal-lokalizuet-odin-iz-etapov-proizvodstva.

177 See, e.g., European Union, "Official Journal of the European Union," Volume 66, June 23, 2023.

178 "Positive Technologies Q2 IFRS revenue rises by 49% to $35.09 mln," *TASS*, July 25, 2023, https://tass.com/economy/1651585.

179 « Группа «Астра» объявила финансовые результаты по МСФО за первое полугодие 2023 года », *C News*, September 22, 2023, https://www.cnews.ru/news/line/2023-09-22_gruppa_astra_obyavila. See also, e.g., « Linux жил, Linux жив, Linux будет жить », *Kommersant*, September 20, 2022, https://www.kommersant.ru/doc/5570730.

180 "Russian Ministry of Digital Development to transform domestic software register into marketplace," *Interfax*, May 25, 2022, https://interfax.com/newsroom/top-stories/79526/.

181 "Domestic Soft Association Asks Ministry of Digital Development not to Ease Entry to Register of Russian Software," ICT Moscow, June 22, 2022, https://ict.moscow/en/news/domestic-soft-association-asks-ministry-of-digital-development-not-to-ease-entry-to-register-of-russian-software/.

182 Natasha Lomas, "Yandex's sale of News and Zen to VK completes," *TechCrunch*, September 12, 2022, https://techcrunch.com/2022/09/12/yandex-news-zen-vk-sale-completes/.

183 Darya Korsunskaya and Alexander Marrow, "Exclusive: Yandex NV could sell Russian assets all at once," *Reuters*, November 14, 2023, https://www.reuters.com/markets/deals/yandex-nv-could-sell-all-russian-assets-one-go-2023-11-14/; "Yandex to Fully Divest Russian Assets and Distribute Proceeds," *Bloomberg*, November 14, 2023, https://www.bloomberg.com/news/articles/2023-11-14/yandex-to-fully-divest-russian-assets-and-distribute-proceeds.

184 "Yandex Announces Third Quarter 2023 Financial Results," Yandex, October 26, 2023, https://ir.yandex/financial-releases?year=2023.

of February 2024, for a sale price of $5.2 billion, this is exactly what Yandex plans to do.[185]

These advances aside, conversations at Positive Hack Days 2023—Russia's largest hacking conference, put on by Russian cyber firm and intelligence contractor Positive Technologies—indicate that many Russian companies are still using Western software even if they are not supposed to do so. There is less visibility into this "shadow" market, but it exists because companies have not always been able to replace foreign-made software with domestic software.[186] A lack of many viable alternatives in kernels, compilers, and interpreters (lower-down parts of the software "stack") contributes to this problem, and it will continue to prove a challenge going forward in building out alternative applications, operating systems, and other technologies in Russia.[187] Compatibility issues also plague Russian-made software. As of June 2023, the Russian government has been creating independent centers to test the compatibility of Russian software with domestic hardware and operating systems for this very reason.[188] It has also announced plans to develop a "Multiscanner" platform to replace the use of VirusTotal, due to Russian government fears that the US government could access data uploaded to VirusTotal via its owner Google.[189]

Russian Tech Investments and Russian-Chinese Tech Entanglement

China is a consistent and growing player in Russia's technology developments. By one count, the economic value of Chinese and Hong Kong exports of US chips to Russia increased ten times from 2021 to 2022 (from $51 million to just under $600 million), and China and Hong Kong comprised nearly ninety percent of global chip exports to Russia between March-December 2022.[190] The US Office of the Director of National Intelligence noted in a declassified June 2023 assessment that "the PRC is providing some dual-use technology that Moscow's military uses to continue the war in Ukraine, despite an international cordon of sanctions and export controls" and cited foreign press reports that Russia has acquired large numbers of chips through small Chinese- and Hong Kong-based traders.[191] Two unnamed senior Biden administration officials said in April 2024 that in 2023, about ninety percent of Russia's microelectronics were provided from China.[192]

In other hardware, Chinese smartphone sales rose forty-two percent by volume in Russia from 2022 to 2023.[193] Chinese smartphone manufacturers Xiaomi and Realme took the first and second spots for Russian market share in 2023, overtaking Samsung (South Korea) and Apple (US).[194] It appears that for some Chinese tech firms, initial concerns about US sanctions and pressure from suppliers[195] have turned into companies remaining in the Russian market. However, there are exceptions when it comes to hardware: Chinese telecom Huawei, for its part, disbanded its enterprise business group in Russia in December 2022 and reportedly stopped taking new contracts to sell network equipment to Russian operators.[196]

Russia's dependence on Chinese technology is less prominent in software. After Visa and Mastercard terminated their business operations in Russia in the spring of 2022,[197] China's UnionPay

185 Alexander Marrow, Darya Korsunskaya, and Polina Devitt, "Yandex owner to exit Russia in a $5.2 billion deal," *Reuters*, February 5, 2024, https://www.reuters.com/technology/yandex-nv-agrees-52-bln-sale-russian-assets-investor-consortium-2024-02-05/.

186 "Network security in Russia: what remains after all is gone," discussion at Positive Hack Days 2023, Moscow, Russia, https://www.youtube.com/watch?v=rxuzvuQrbC0.

187 "Cyber sovereignty: open code contribution," discussion at Positive Hack Days 2023, Moscow, Russia, https://www.youtube.com/watch?v=nj3KqTVPza4.

188 "Russian Software: Domestic Software," TA Adviser, July 18, 2023, https://tadviser.com/index.php/Article:Russian_Software_(Domestic_Software).

189 Alexander Martin, "Russia to launch its own version of VirusTotal due to US snooping fears," *The Record*, October 30, 2023, https://therecord.media/russia-launching-own-malware-repository-virustotal.

190 Brian (Chun Hey) Kot, "Hong Kong's Technology Lifeline to Russia," Carnegie Endowment for International Peace, May 17, 2023, https://carnegieendowment.org/2023/05/17/hong-kong-s-technology-lifeline-to-russia-pub-89775.

191 "Support Provided by the People's Republic of China to Russia," US Office of the Director of National Intelligence, June 2023, 6, https://democrats-intelligence.house.gov/uploadedfiles/odni_report_on_chinese_support_to_russia.pdf.

192 "US intelligence finding shows China surging equipment sales to Russia to help war effort in Ukraine," *The Associated Press*, April 19, 2024, https://apnews.com/article/united-states-china-russia-ukraine-war-265df843be030b7183c95b6f3afca8ec.

193 Iris Deng, "Chinese smartphone brands gain market share in Russia with Xiaomi gaining top spot displacing Samsung," *South China Morning Post*, April 18, 2023, https://www.scmp.com/tech/big-tech/article/3217430/chinese-smartphone-brands-gain-market-share-russia-xiaomi-gaining-top-spot-displacing-samsung.

194 Ibid.

195 See, e.g., Dan Strumpf, "Chinese Tech Giants Quietly Retreat From Doing Business With Russia," *The Wall Street Journal*, May 6, 2022, https://www.wsj.com/articles/chinese-tech-giants-quietly-stop-doing-business-with-russia-11651845795.

196 Iris Deng, "Huawei disbands enterprise business team in Russia in further pullback amid Western sanctions, local media reports," *South China Morning Post*, December 20, 2022, https://www.scmp.com/tech/big-tech/article/3203995/huawei-disbands-enterprise-business-team-russia-further-pullback-amid-western-sanctions-local-media; "Huawei," KSE Institute, accessed January 21, 2024, https://leave-russia.org/huawei.

197 "Visa Suspends All Russia Operations," Visa, March 5, 2022, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.18871.html#:~:text=SAN%20FRANCISCO%2D%2D(BUSINESS%20WIRE,transactions%20over%20the%20coming%20days.; "Mastercard statement on suspension of Russian operations," Mastercard, March 5, 2022, https://www.mastercard.com/news/press/2022/march/mastercard-statement-on-suspension-of-russian-operations/.

system was briefly seen as an alternative before it stopped accepting cards from sanctioned Russian banks in September 2022.[198] OpenKylin, China's first domestic-made open-source operating system for desktops, built on Linux, was released in July 2023—but it is unclear how much it might be presently used in Russia.[199] As mentioned, Russia has been developing the Astra Linux operating system—which is also based on Linux and has an open-source version—as a replacement for Microsoft Windows.[200] The state banned officials from using foreign-built messaging apps in March 2023, including the Chinese platform WeChat (along with Telegram, WhatsApp, and others).[201] Russian authorities are also looking to develop a Russian app that, similar to WeChat, serves as a one-stop-shop for communications, banking, and more—and which could enable, much like WeChat, a dangerous kind of concentrated surveillance.[202]

On the investment front, the Russian Ministry of Economic Development quoted a Chinese representative in November 2022 stating that Chinese investment in Russia from January to August of 2022 totaled $450 million, up 150 percent from the same period in 2021.[203] But this investment has not been consistent across sectors or as meaningful in the technology realm. Analysis from the Observer Research Foundation, an India-based think tank, found that Chinese investment in Russia has "surged" in the energy, infrastructure, and transportation sectors—while "fear of Western sanctions has driven away major Chinese tech companies such as Huawei and DJI from Russia, much to the chagrin of Moscow."[204] Former Russian journalist and economics expert Mikhail Korostikov has also argued that Chinese investment in Russia "remains relatively small, partly because Moscow is not prepared to accept Chinese investment without certain restrictions."[205] An analysis from the Asia Society in October 2023 concluded that "Beijing is in no hurry to embed itself in the unpredictable and now war-focused and strained Russian economy" as investment flows stay "modest."[206] Russian dependence on Chinese technology in some areas, such as semiconductors, does not necessarily translate to other areas such as software usage and investment.

On the domestic financing front, the National Technology Initiative, first called for by Putin in 2014 and established formally in 2016, currently has sixty-eight projects approved under its general NTI Fund, one of the multiple vectors through which the state financially supports projects focused on high-tech industries.[207] Most projects are, as of July 2023, in the implementation stage, with others suspended, discontinued, or undergoing post-project monitoring.

198 Selena Li, "Explainer: China UnionPay, Russia's potential payments backstop," *Reuters*, April 21, 2022, https://www.reuters.com/business/finance/china-unionpay-russias-potential-payments-backstop-2022-04-21/; Nicholas Gordon, "Visa and Mastercard have already cut ties with Russian banks. Now China's largest credit card brand might be pulling out too," *Fortune*, April 22, 2022, https://fortune.com/2022/04/22/unionpay-china-credit-card-sberbank-secondary-sanctions-russia/; "Chinese UnionPay System Cuts Off Russian Bank Cards," *Kyiv Post*, September 3, 2022, https://www.kyivpost.com/post/1439.

199 Josh Ye, "China releases its first open-source computer operating system," *Reuters*, July 6, 2023, https://www.reuters.com/technology/china-releases-its-first-open-source-computer-operating-system-2023-07-06/; Tao Mingyang, "China's homegrown operating system sees rapid development as US' tech assault backfires," *Global Times*, August 10, 2023, https://www.globaltimes.cn/page/202308/1296031.shtml.

200 Catalin Cimpanu, "Russian military moves closer to replacing Windows with Astra Linux," *ZDNet*, May 30, 2019, https://www.zdnet.com/article/russian-military-moves-closer-to-replacing-windows-with-astra-linux/; "Digital Ministry drafting changes to allow developers to participate in international projects not registered in Russia," *Interfax*, October 11, 2023, https://interfax.com/newsroom/top-stories/95329/.

201 Phil Muncaster, "Russian Government Bans Foreign Messaging Apps," *Infosecurity*, March 2, 2023, https://www.infosecurity-magazine.com/news/russian-government-bans-foreign/.

202 Mike Eckel, "One App To Rule Them All: Coming Soon To Russia's Internet," *Radio Free Europe/Radio Liberty*, December 2, 2023, https://www.rferl.org/a/russia-internet-app-social-media-surveillance-/32711114.html. See also, Philipp Dietrich, "The Key Player in Russia's Cybersphere," German Council on Foreign Relations, September 2023, https://dgap.org/en/research/publications/key-player-russias-cybersphere.

203 The original Russian government webpage, linked in the story by *Kommersant*, is not accessible. « Россия и Китай договорились проинвестировать совместные проекты на $1,3 млрд », *Kommersant*, November 8, 2022, https://www.kommersant.ru/doc/5652855. See also Russian government discussion of Russian-Chinese trade: "Andrei Belousov: Trade in Russia and China can reach $300 billion by 2030," Government of Russia, November 20, 2023, http://government.ru/en/news/50157/.

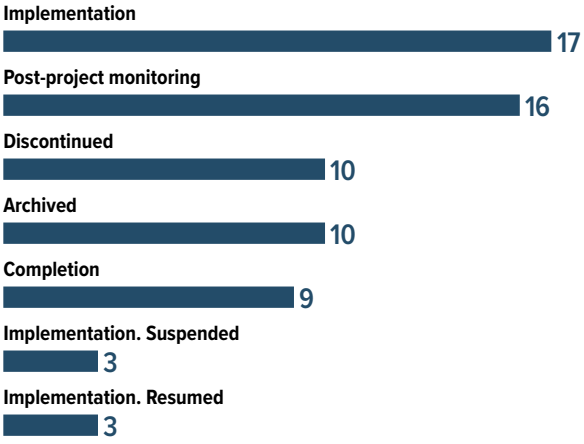
204 Prithvi Gupta, "China's steadily expanding investments in Russia since the Ukraine conflict," Observer Research Foundation, July 26, 2023, https://www.orfonline.org/expert-speak/chinas-steadily-expanding-investments-in-russia-since-the-ukraine-conflict.

205 Mikhail Korostikov, "Is Russia Really Becoming China's Vassal?" Carnegie Endowment for International Peace, June 7, 2023, https://carnegieendowment.org/politika/90135.

206 Philipp Ivanov, "Together and Apart: The Conundrum of the China-Russia Partnership," Asia Society, October 202), https://asiasociety.org/policy-institute/together-and-apart-conundrum-china-russia-partnership.

207 « Реестр проектов », NTI 2035, accessed September 25, 2023, https://nti2035.ru/catalog/.

FIGURE 2: RUSSIA NATIONAL TECHNOLOGY INITIATIVE-APPROVED PROJECTS BY STATUS (AS OF JULY 2023)



Data Source: National Technology Initiative, July 28, 2023.

The list goes on. Russia's National Technology Initiative announced a new project in April 2023, called NTI Venture Funding, in partnership with the Popov Radio Manufacturing Plant in Siberia. Reportedly, the NTI Venture Funding project plans to invest approximately $65.8 million in 20 or more projects across robotics, microelectronics, unmanned aviation, cargo delivery, and wireless technology, among others.[208] It is clear that developing Russian alternatives to foreign tech remains the goal. In practice, this venture funding plan contrasts with overall Russian spending on R&D, which as indicated above has remained stagnant for two decades. For 2024, the Russian government plans to spend six percent of GDP on the military, most of which will likely go towards the production of military equipment.[209] Some technology companies may be able to pitch defense- and military-focused projects to receive some of the funding, such as "information security" systems for combat units. But even that sub-slice of the pie, if it materializes at all, is hardly enough to catapult Russia's digital tech development and commercialization to the levels once imagined a decade prior.

The drumbeat of restrictions, meanwhile, continues: in September 2022, Putin declared that the government must ensure Russia's technological independence from foreign software by December 2022;[210] in August 2023, Putin signed a new law banning state agencies and companies from using non-Russian and non-compliant geoinformation technologies, beginning in January 2026.[211] It is often unclear how these deadlines are set and whether they are remotely realistic. Simultaneously, the Putin regime's obsessive focus on defense and securitization may increase the likelihood that new digital technologies developed in Russia are grabbed up by the military and defense base before companies or scientific research centers have opportunities to develop the commercial or civilian use that would increase their sustainability and attract investment.

CONCLUSION AND KEY TAKEAWAYS

Russia's technological independence was an idea accelerated into reality by the conspiratorialism and paranoia surrounding the early 2000s "color revolutions" in former Soviet republics and the Kremlin's "internet awakening" in the late 2000s and early 2010s. Now, Russia's digital isolationism is both a growing reality and an explicit goal of the state. In some ways, this evolving saga appears to corroborate what economist Sergei Guriev argued in 2015:

> *"Having understood that its current foreign policy can only lead to isolation, the Russian government has put together a narrative in which this was its plan all along—that isolation is actually good for Russia. By reducing imports and foreign investment, the government claims that sanctions and countersanctions will eventually promote import substitution and growth."* [212]

The Kremlin is now further locked into this narrative, complemented by a loud (but bogus) narrative of Russia's "victimization" by Western sanctions, cyber operations, and critical news reporting (As of late, Moscow calls reporting on the war it dislikes "information operations" or "information war"). Even Vladimir Putin, in a May 2022 Russian Security Council meeting, said that "a number of Western tech companies unilaterally cut off Russia from technical support services for their equipment" and that "all this should be taken into account when Russian companies

208 "Russia Forms Drone, Microchip Investment Fund – *Vedomosti*," *The Moscow Times*, April 3, 2023, https://www.themoscowtimes.com/2023/04/03/russia-forms-drone-microchip-investment-sovereign-fund-vedomosti-a80688; « В России появился венчурный Фонд суверенных технологий », *Vedomosti*, April 3, 2023, https://www.vedomosti.ru/technology/articles/2023/04/03/969178-v-rossii-poyavilsya-venchurnii-fond-suverennih-tehnologii.

209 Emma Burrows, "A record Russian budget will boost defense spending, shoring up Putin's support ahead of the election," *The Associated Press*, November 15, 2023, https://apnews.com/article/russia-draft-budget-state-duma-economy-ukraine-4ac21a2259169d7c689ac452830bb0af; Pavel Luzin and Alexandra Prokopenko, "Russia's 2024 Budget Shows It's Planning for a Long War in Ukraine," Carnegie Endowment for International Peace, November 10, 2023, https://carnegieendowment.org/politika/90753.

210 "Putin instructs Cabinet to take steps to make Russia independent from foreign software," *TASS*, September 5, 2022, https://tass.com/politics/1502743.

211 « Подписан закон о переходе на использование отечественных геоинформационных технологий », *Digital Russia*, August 7, 2023, https://d-russia.ru/podpisan-zakon-o-perehode-na-ispolzovanie-otechestvennyh-geoinformacionnyh-tehnologij.html.

212 Sergei Guriev, "Deglobalizing Russia," Carnegie Endowment for International Peace, December 2015, 3, https://carnegieendowment.org/files/Article_Guriev_Eng.pdf.

and public authorities introduce new foreign IT products or use previously installed ones."[213] Narratives aside, the recognition is there: Russia's technological autonomy has always been a goal, and its relative technological isolation is now a growing reality.

This section is geared toward at least four groups of policymakers and government organizations:

- The State Department, the US Agency for International Development (USAID), and others working on multilateral technology relations and capacity-building, founded on an understanding of Russia's current technological ecosystem.
- US and Western intelligence organizations monitoring the development of Russia's technology sector as well as Russia's offensive cyber capability development, technology procurement, and relationships with China.
- Those at the US Bureau of Industry and Security (BIS) under the Department of Commerce and others seeking to understand Russian demands for technologies that are export-controlled (e.g., semiconductors) and Russia's level of technological independence versus dependence on foreign suppliers and investors.
- US, allied, and partner defense and security policymakers with an overall interest in evaluating how the 2022 Russian war on Ukraine has impacted Russian technology.

Key Takeaways and Recommendations

1. **Russia has even fewer incentives (and even less room) today to stop pursuing an isolationist and securitized approach to digital technology—which will have impacts across international tech engagement, domestic policy, and human rights.** The waves of sanctions against Russia and the termination of many tech relationships with Russian firms have cemented this as a reality for the Kremlin and Russian industry. Sanctions and terminated business relationships likely serve as confirmation bias for Russian officials who believe that a military and security paradigm is the most important and realistic way to approach technology development, deployment, and governance.[214] After all, one vein of argument goes, if the US and the West are going to weaponize technology in their favor and to Russia's detriment, Russia must approach technology through a securitized lens. US officials should remember that this is not purely a propagandistic line. Despite some analysts dismissing Russian worries about Western tech—characterizing them as bad-faith arguments made for utilitarian purposes—Russian officials' concerns about foreign technology are genuine and serious in that they truly believe Western technology is a source of foreign election meddling, disinformation, espionage, and sabotage in Russia.[215] This is all the more interesting as Russia becomes more digitally dependent on China.

   - **The State Department and USAID, among other organizations,** should continue evaluating how this momentum for isolating and securitizing digital technology will harm freedom of expression and further impede opportunities for Russians to dissent in the country. Russian tech platforms and services will have more surveillance and censorship built in than most Western alternatives, such as YouTube or the encrypted messaging app Signal. For example, the push to develop a super app in Russia[216]—one where payments, communications, and other functions are embedded into one application, much like China's WeChat—is potentially a surveillance nightmare in the hands of an ever-more paranoid and security-driven regime. Some Russians and analysts have also worried the Kremlin will block YouTube in the coming months.[217] Capacity-building, development, and freedom of expression efforts focused on Russia and the region will need to increase investments in virtual private networks (VPNs) and other means of providing access to less-censored and surveilled platforms for the Russian people. The highly dynamic nature of the surveillance risks on the Russian internet (such as how VPNs are monitored and blocked or which organizations take charge of policing which kind of dissent) requires capacity-building agencies and democracy-focused nongovernmental organizations to continuously engage those with on-the-ground insights into Russia's censorship, surveillance, and tech isolation.

213 "Security Council Meeting," The Kremlin, May 20, 2022, http://en.kremlin.ru/events/president/news/page/65.

214 See, e.g., Gregory Arcuri, "Lessons from Russia's Dysfunctional Pre-War Innovation Economy," Center for Strategic & International Studies, April 11, 2022, https://www.csis.org/blogs/perspectives-innovation/lessons-russias-dysfunctional-pre-war-innovation-economy ("…Putin's regime has been at best indifferent—and at worst, hostile—towards the civilian and purely economic application of emerging technologies.")

215 See, e.g., on the dismissal of these concerns, Jon Fingas, "Russia is ditching Microsoft because it's an easy target," *Engadget*, July 18, 2019, https://www.engadget.com/2016-11-02-russia-to-drop-microsoft-software.html.

216 Eckel, "One App To Rule Them All: Coming Soon To Russia's Internet."

217 See, e.g., Philipp Dietrich, "Banning YouTube in Russia: Just a Matter of Time," German Council on Foreign Relations, April 4, 2024, https://dgap.org/en/research/publications/banning-youtube-russia-just-matter-time-0; "Russia To Create Blacklist Of YouTube Vloggers Who Refuse To Join Kremlin-Backed Platform," *Radio Free Europe/Radio Liberty*, February 10, 2024, https://www.rferl.org/a/russia-youtube-blacklist-vloggers/32813744.html; Author's conversation with an expert in Russia's technology ecosystem. See the state's denial from 2022, with relative silence since: "Russia Will Not Ban YouTube, Minister Shadayev Says," *Radio Free Europe/Radio Liberty*, May 17, 2022, https://www.rferl.org/a/russia-ban-youtube-shadayev/31854787.html.

- **The State Department, the intelligence community, and other elements of US and allied and partner governments working on Russia issues** should seriously weigh their assumptions about Russian thinking against the evidence that Russian officials are genuine in their characterization of the internet as a weapon and a threat—and Western technologies as a threat to regime security and tools of foreign subversion. Analysts and policymakers should not underestimate the extent to which ideology, more than economic aims, drives Russian technology and information actions.[218]

2. Russian companies have shown more success building their own domestic software than domestic hardware. Domestic software competitors have existed for years in areas like search (Yandex) and social media (VK and Odnoklassniki, or OK, which is also now owned by VK). The Astra Linux operating system is slowly but surely used on more and more government systems as well as private systems in industries like healthcare. For all the struggles facing the state—such as continued dependence on non-Russian technology and Russian companies "shadow" installing non-Russian technology without the state's knowledge, or at least with its blind eye—the success story here is a greater possibility than it is with domestic hardware. On that front, Russia's microelectronics manufacturing capability remains wholly insufficient. The US and its Western allies and partners have already seriously constrained Russia's microelectronics sector—as have companies like TSMC—by simply ending their business relationships in the country. Russia cannot produce viable chips and other technology at any scale to be meaningfully useful. The country has become more dependent on Chinese hardware, and intelligence services have had to lean into the theft of processors and other hardware from the West. Russia's hardware activities in the coming years are most likely to focus on illicit procurement rather than attempting to stand up domestic manufacturing capabilities (which the state has struggled to do for years). These challenges are exacerbated by a lack of investment: Russia's spending on domestic R&D has hovered around one percent from 2000-2020. Those numbers are unlikely to shift as the state focuses its resources on the war in Ukraine and the immediate military uses of digital technology. The state has announced some plans to increase venture funding for Russian companies but is unclear how that will unfold—especially as most venture funding will not fix the immediate, underlying issue of the country's minimal hardware manufacturing capacity.

- **BIS and other agencies monitoring export controls and Russia's interest in illicit technology procurement** should continue to monitor public reporting about Russian software, firmware, and hardware development—and also make sure to integrate some of the investment data, news sources, Russian industry discussions, and other references cited in this report into their analysis. Ever since the Putin regime began its strong push to boost Russian domestic technology and reduce technological dependence on the West, there have been important gulfs between government policy, on-the-ground reality, and what industry leaders have thought versus said aloud. Those gaps, which can often come to light in Russian news reporting and Russian industry conversations, provide critical insights into where the Russian government might move next. For instance, Russian companies' past complaints about nonfunctional chips spoke to some of the underlying, systemic issues Russia faces with semiconductor manufacturing. The latest industry excitement about an Astra Linux technology stack, by contrast, speaks to greater advancements when it comes to operating systems, also made clear by news reports and other information. In addition to nonpublic information sources, these conversations and sentiments should not be overlooked. Rhetoric from state officials should be matched against industry conversations and the most reliable data on state and commercial investment in digital technology R&D. US policymakers should use the reality of investment (and lack thereof) in Russian domestic digital tech, rather than just state policy, to understand Russia's future directions.

- **The US defense and intelligence community, as well as those of US allies and partners,** should note that technological isolation poses new or enhanced cybersecurity risks to the Russian state. For example, on the domestic software side, widespread use of the Astra Linux operating system and the company's goal of creating a full-fledged software stack[219] potentially create new single points of failure and concentrations of technology that the West could exploit. US allies and partners may also wish to track and analyze these domestic digital technology concentrations to evaluate where they may create new vulnerabilities.

- **BIS and its Commerce Department partner agencies, the State Department, and others tracking Russia's domestic software development** should monitor new developments in the Russian private sector and hacking community to understand future directions across operating systems, mobile apps, and other technology and software. These developments matter for Russia's tech sector at home, its ability to market products and services overseas, and the technical vulnerabilities within Russian networks. Still, whether the Russian state can and will muster the resources, bureaucratic buy-in, and industry coordination to promote

218 Thanks to Iria Puyosa for further discussion of this point.

219 « Мы строим глобального вендора системного ПО », *C News*, 2021, https://www.cnews.ru/projects/2021/astra_linux.

domestic software is an open question. As Russian journalist and intelligence expert Andrei Soldatov notes, "The concept of [domestic software] registers also encompasses the fundamental belief in the possibility of forming a final, exhaustive list of everything, from innovation to enemies of the regime."[220] Mandating licensing processes and other checks before deploying even the most basic software can also slow down implementation.[221] Such considerations should guide how US and allied governments issue sanctions and investigate sanctions evasion—and agencies can assess these challenges by monitoring what Russian companies, hackers, and developers are publicly saying on blogs and at conferences and events.

3. **The Russian cybersecurity sector will play an important role in Moscow's reaction to growing sanctions and other restrictions as well as its efforts to technologically isolate itself from the West**. Russian cybersecurity companies are dealing with a complex landscape at home. There is a nuanced spectrum of perspectives within the industry on Western sanctions, the 2022 Russian war on Ukraine, and the Putin regime's domestic tech push—and many of these individuals are in difficult positions remaining in the country. While some companies and individuals are vocally supportive of the state's propaganda and its domestic tech pushes, even those perspectives may come from a genuine belief in the state's narratives, a desire to appear supportive of state efforts, or self-serving wishes to profit off the domestic tech push, tax subsidies, and other newly introduced policies from the Russian government. Many other firms may express agreement with state policies when that does not actually reflect their view.[222] The security-focused nature of some of these companies, albeit often in a commercial and consumer-protective sense, may still give them more rhetorical play with Moscow than other tech companies outside the "defensive" sphere.

   - **US and Western policymakers** generally trying to understand the future of Russia's tech sector—whether to evaluate sanctions efficacy (e.g., at BIS), track emerging cyber threats (e.g., at the UK's National Cyber Security Centre), or something else entirely—should know that there is increasingly little room within Russia's technology sector to push back against the state or to contradict core Kremlin objectives, such as getting rid of Microsoft Windows in state organizations and "critical information infrastructure" operators. But, to recall historian Stephen Kotkin's quote, binaries are not an effective way to understand Russia. The state does not control every single tech decision in the country, and in many areas, the state does not have or has not demonstrated high competence on technical issues, such as with building cyber defense systems. Within the space that companies do have to push back or shape initiatives, cybersecurity companies providing services to the state and the security services will be an important voice in how some of these policies are designed and implemented; the Ministry of Digital Development does at least speak with and listen to their perspectives. That some of these companies are adjacent to or squarely within the national security sphere will help their influence in a state increasingly dominated by conspiratorial, paranoid, and security-driven views of technology. Western organizations should be sure to monitor public sources from Russian cybersecurity companies, forums, and conferences to gain these insights.

4. **Some Russian technology companies are already looking to the international market to expand their profit streams, including in internet and cybersecurity services, or to separate their Russian components entirely.** Yandex had been discussing the possibility of splitting the company into two parts since Russia's full-scale invasion of Ukraine, one of which would operate within Russia and the other internationally. This effort is ongoing but faces many challenges, given the sheer number of Yandex employees and developers alone who appear to be based in Russia[223] and the government's interference with the restructuring due to anti-war comments made by Yandex's co-founder.[224] Nonetheless, negotiations held at the end of 2023 drive this corporate restructuring closer to reality. Some of the leaders in Russia's cybersecurity sector, meanwhile, remain globally competitive. For instance, the revenue of Positive Technologies, a US-sanctioned firm that supports Russia's intelligence community, has only been growing internationally in the last two years despite the ongoing war. In July 2023, the company announced that it had shipped forty-six percent more prod-

220 Andrei Soldatov, "Russia's Endless Registers Are a Back Door to Preliminary Censorship," *The Moscow Times*, June 29, 2021, https://www.themoscowtimes.com/2021/06/29/russias-endless-registers-are-a-back-door-to-preliminary-censorship-a74376.

221 See, e.g., the comments quoted in: Hillenius, "Russia scrapped open source plans to focus on self-reliance."

222 Justin Sherman, "Russia's largest hacking conference reflects isolated cyber ecosystem," Brookings Institution, January 12, 2023, https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.

223 Justin Sherman, "Analyzing Russian Internet Firm Yandex, Its Open-Source Code, and Its Global Contributors," Margin Research, March 27, 2023, https://margin.re/2023/03/analyzing-russian-internet-firm-yandex-its-open-source-code-and-its-global-contributors/.

224 "Russia Revises Yandex Partition Terms Over Founder's Anti-War Stance – Reports," *The Moscow Times*, October 6, 2023, https://www.themoscowtimes.com/2023/10/06/russia-revises-yandex-partition-terms-over-founders-anti-war-stance-reports-a82686.

ucts and services compared to the prior year, to the tune of approximately $47.6 million.[225]

- **The State Department and other organizations** building and engaging on US global technology policy should not dismiss the notion of Russian cyber firms remaining globally competitive—thinking of companies like Kaspersky or Positive Technologies as industry *persona non grata* post-February 2022. That would be a mistake. Analysts should watch how companies like Positive Technologies are positioning themselves to compete in overseas markets, ranging from Latin America to the Asia-Pacific, in some cases by explicitly offering themselves as alternatives to Western technology and ways for organizations to decentralize their risk. You might be concerned about Russian tech, the pitch goes, but you certainly do not want to rely entirely on US, Israeli, or Chinese cyber solutions, either; using domestic tech in some areas and theirs in others is a way to minimize exposure to both.[226] Many of these companies are primarily commercially motivated but still operate within an increasingly constrained Russian political environment. Their expansion can therefore serve as a means by which Moscow can project influence, gather data, and engage in other activities as well.

- **The State Department and the defense and intelligence community** should also observe the growth of Russian internet firms like Yandex which may receive skepticism or face restrictions in some parts of the world (e.g., Western Europe) but may offer attractive cloud and other services elsewhere (e.g., Latin America). For Yandex, this is especially the case if its deal goes through to sell the Russian business entity to Russian managers and oil company Lukoil for $5.2 billion.[227] The Dutch parent could then run Yandex's current, non-Russian business operations separately. (Of course, this will further harm human rights in Russia and expand the Kremlin's domestic internet control as the Russian Yandex falls further under the state's grip.)[228] US analysts and policymakers should track these developments and prepare for this reality, also potentially noting to US companies that they will still be competing with Russian or historically Russian internet and cyber firms in certain parts of the world.

5. Russia is becoming more digitally dependent on China. Chinese digital technology has long played a part in Russia's domestic technology evolution, such as in the failed Skolkovo Innovation Center, but dependence is at newly high levels. Western sanctions, Western businesses exiting the country, IT workers fleeing Russia, and the Putin regime's even greater paranoia about Western digital technology, among other factors, have increased Russia's reliance on Chinese chips, software, and other technology. The Russian government is concerned about this dependence—despite what one might assume, there are Russian security analysts worried about espionage and digital threats from Beijing, too. But it has little choice in the face of digital techno-isolationism and serious problems with domestic, digital technology development and procurement. This digital dependence on China has accelerated since February 2022. Russia's increasing use of Chinese software and especially hardware should change how the US strategically and tactically approaches China, Russia, countries concerned about Beijing and Moscow's tech activities, and the tech ecosystem in Russia.

- **The White House and the State Department** should, at the strategic level, evaluate existing policies and plans against Moscow's growing digital dependence on China—and determine how that dependence could or should shift the US' approach to countering Beijing's global technology influence and its efforts to acquire technology from the West. For instance, for countries around the world that are more concerned about Russian government activities than Chinese government activities, this trend highlights how the two issues are entangled. If Chinese technology is facilitating Russia's technological influence or military and intelligence activities, countries worried about Moscow may become more concerned about Chinese government tech programs and policies. This trend may also change how US diplomats engage with or signal to Russia: Kremlin officials are certainly most worried about espionage, information warfare, and regime security threats from the West, but that doesn't mean they are fearless about using Chinese technology. And somewhat unlike their Chinese counterparts, who integrate commercial and economic views into their perception of the security of digital technologies, Moscow is much less focused on the economics of digital technologies and much more driven by a conventional security lens.

- **The White House, State Department, and Defense Department** should note that for all Putin and Chinese leader Xi

225 « Бизнес Positive Technologies растет: компания увеличила объем отгрузок во втором квартале на 71% — до 3,3 млрд рублей », PT Security, July 25, 2023, https://group.ptsecurity.com/ru/news/biznes-positive-technologies-rastet-kompaniya-uvelichila-obem-otgruzok-vo-vtorom-kvartale-na-71-do-3-3-mlrd-rub.

226 « Positive Technologies: Вероятна международная экспансия », IT Invest, June 9, 2022, https://itinvest.ru/analytics/stocks/stocks-ideas/12861/.

227 David McHugh, "The owners of Russia's tech pioneer Yandex are selling — at a big, Kremlin-required discount," *The Associated Press*, February 5, 2024, https://apnews.com/article/yandex-russia-sale-search-engine-4de5a04fcf9b99ed5b5fc5fcdd24dd2a.

228 See, e.g., Anton Shvets, "The sale of Yandex is a weapon in the hands of the Kremlin," *Ukrainska Pravda*, March 21, 2024, https://www.pravda.com.ua/eng/columns/2024/03/21/7447514/.

Jinping may cooperate in some areas,[229] elements of the Russian state worry about Chinese tech dependence.[230] In the summer of 2022, for instance, an internal Russian Ministry of Digital Development assessment expressed senior officials' concern about the dominance of Chinese companies like Huawei in Russia and the resulting information security risks.[231] Russian officials proposed imposing quotas on Chinese tech imports, shifting production of certain components to Russia, and using Russian subcontractors to limit direct and total dependence on China.[232] Even since the 2022 Russian war on Ukraine began, Chinese government-linked threat groups have been publicly tied to espionage campaigns against Russian defense institutions.[233] The US may wish to shape its communications and signaling to Moscow with that in mind.

- **The US defense and intelligence community, as well as those of US allies and partners,** should consider at the tactical level how Russia's growing digital dependence on China may create new points of vulnerability. This could lead to opportunities for the US and its allies and partners to continue mapping the technological environment in Russia and explore how capabilities could be applied to intelligence and other advantages.

ABOUT THE AUTHOR

Justin Sherman is a nonresident fellow at the Atlantic Council's Cyber Statecraft Initiative. He is also the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm; an adjunct professor at Duke University's Sanford School of Public Policy; and a contributing editor at Lawfare. He writes, researches, consults, and advises on Russia security and technology issues and is sanctioned by the Russian Ministry of Foreign Affairs.

ACKNOWLEDGMENTS

The author would like to thank Gavin Wilde, Carolina Vendil Pallin, Trey Herr, Jackie Kerr, Michael van Landingham, Emma Schroeder, Dylan Myles-Primakoff, Iria Puyosa, Konstantinos Komaitis, and Andrew D'Anieri for their comments on earlier drafts of this report—and Nitansha Bansal for critical help in getting the report to final form.

229 See, e.g., Karen DeYoung and Missy Ryan, "Russia says China agreed to secretly provide weapons, leaked documents show," *The Washington Post*, April 13, 2023, https://www.washingtonpost.com/national-security/2023/04/13/russia-china-weapons-leaked-documents-discord/.

230 Even beyond cyber per se, Elizabeth Wishnick argues that the "Russian intelligence services have been increasingly uneasy about the scope of Chinese intelligence-gathering in Russia, even publicizing cases of Russians being apprehended for spying for China." See: Elizabeth Wishnick, "A 'Superior Relationship': How the Invasion of Ukraine Has Deepened the Sino-Russian Partnership," *China Leadership Monitor* 76 (June 2023), https://www.prcleader.org/post/a-superior-relationship-how-the-invasion-of-ukraine-has-deepened-the-sino-russian-partnership.

231 Alberto Nardelli, "Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech," *Bloomberg*, April 18, 2023, https://www.bnnbloomberg.ca/russian-memo-said-war-leaves-moscow-too-reliant-on-chinese-tech-1.1909355.

232 "Sanctions-Hit Russia Wary of Over-Reliance on Chinese Tech — *Bloomberg*," *The Moscow Times*, April 19, 2023, https://www.themoscowtimes.com/2023/04/19/sanctions-hit-russia-weary-of-over-reliance-on-chinese-tech-bloomberg-a80875.

233 "Twisted Panda: Chinese APT Espionage Operation Against Russian State-Owned Defense Institutes," CheckPoint, May 19, 2022, https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Alain Bejjani
Colleen Bell
Sarah E. Beshar
Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ankit N. Desai
Dario Deste
*Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Stuart E. Eizenstat
Tara Engel
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Francesco G. Valente
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of April 24, 2024

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org