Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia's Repressive Capacities

Burkhardt, Fabian; Wijermars, Mariëlle

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Burkhardt, F., & Wijermars, M. (2022). Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia's Repressive Capacities. *The SAIS review of international affairs*, *42*(2), 21-43. https://doi.org/10.1353/sais.2022.0009

Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia's Repressive Capacities

Fabian Burkhardt and Mariëlle Wijermars

Original publication	SAIS Review of International Affairs
ISSN	1945-4724 1945-4716 (Print)
Volume/Year	Vol. 42, No. 2 (Summer-Fall 2022)
Pages	21 – 43
DOI	10.1353/sais.2022.0009
Publisher	John Hopkins University Press
Recommended citation	Burkhardt, Fabian and Mariëlle Wijermars. "Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia's Repressive Capacities." SAIS Review of International Affairs, vol. 42 no. 2, 2022, p. 21-43. Project MUSE, doi:10.1353/sais.2022.0009.

Further notes on this version

- Original pagination in bold squared brackets (e.g. **[page 28]**)

Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-induced Infrastructural Disruptions are Reshaping Russia's Repressive Capacities

Fabian Burkhardt and Mariëlle Wijermars

Advances in digital technology are fundamentally reshaping the nature and dynamics of control mechanisms in authoritarian states. While there has been a surge in research on the strategies autocracies use to enhance control over the internet, scholarship on "digital authoritarianism" insufficiently acknowledges the concentration of power in increasingly integrated digital infrastructures and the transnational dependencies this has given rise to. In this article we argue that authoritarian states' dependence on foreign digital technologies and services can shape and constrain their capacity to control, surveil, and repress domestically. To illustrate our argument, we examine how Russia's war against Ukraine and the sanctions imposed on Russia in response have influenced its domestic repressive capacities. Assessing the period February-September 2022, we find that the war has had an ambiguous effect, both providing enhanced capacity for digital authoritarianism and undermining the future integrity of the digital infrastructures on which this repressive apparatus relies on.

Introduction

Advances in digital technology are fundamentally reshaping the nature and dynamics of control mechanisms in authoritarian states. While both scholarly debate and foreign policy practice initially placed high hopes on the democratizing potential of the internet,[1][2][3] the proliferation of internet access has instead given rise to "networked" or "digital" authoritarianism: a condition in which autocrats promote digitalization and allow online discourses to develop, which provides leaders with novel ways of monitoring and influencing their population and thwarting challenges to their rule.[4][5] As numerous stud- **[page 21]** ies have demonstrated, digitalization may in fact strengthen—rather than weaken—authoritarian regimes.[6][7][8] Referring to the cases of Russia and Hungary, Sergei Guriev and Daniel Treisman claim that a new type of autocracy has emerged. Rather than relying on ideology or the use of force, these "informational autocracies" survive by "manipulating public opinion."[9] Controlling information flows, including those online, therefore becomes paramount.

There has been a surge in research demonstrating the variety of strategies autocracies employ to enhance their control over the digital sphere and the reasons why autocrats choose (not) to restrict digital freedoms.[10][11][12][13] Yet scholarship has largely overlooked one key element: the concentration of power in increasingly integrated digital infrastructures and the resulting transnational dependencies. In this article, we demonstrate how, as a result of this, the deepening reliance on digital technologies introduces novel constraints upon authoritarian practices that mitigate their effectiveness. Few countries aside from the US and China can claim to be fully

"sovereign" in terms of their digital infrastructures, technologies, and content. While some countries (such as Russia, South Korea, and India) balance domestic and foreign providers, most are dependent on foreign platforms, software, and hardware providers. As such, these countries remain vulnerable to the regional and global influence of dominant technological powers.[14] Foreign ownership of intrastructure may significantly decrease the capacity of authoritarian leaders to leverage control. For example, internet shutdowns or online censorship are often facilitated through state ownership or informal control of privately held infrastructures.[15][16] To fully understand digital authoritarianism today, it is essential to examine these dependencies and their geopolitical dimensions.

The issue of globalized digital infrastructures and their geopoliticization has recently gained currency within the discipline of international relations through the concept of "weaponized interdependence" proposed by Henry Farrell and Abraham L. Newman.[17] This concept posits that the asymmetry of globalized economic networks, including the internet, enables states who control key *choke points* to exert control over other states' behavior in novel ways. For example, states can achieve an informational advantage when they have "physical access to or jurisdiction over hub nodes" such as internet cable landing sites or use their network centrality to "limit or penalize" the use of these hub nodes by third parties.[18] However, the research has not yet tackled the implications of the concept on the dynamics of digital authoritarianism (i.e., its *domestic* dimensions). To advance this direction for research and illustrate our core argument, we examine the case of Russia; a country characterized by **[page 22]** a digital semi-dependency exacerbated by recent technological sanctions. Examining the case of Russia over the period from February to September 2022 allows us to elucidate the structural constraints and vulnerabilities resulting from transnational digital dependencies. We ask: how is Russia's war against Ukraine and the sanctions imposed in response to it influencing digital authoritarianism in Russia?

We take heed of criticism on how Farrell and Newman conceptualize states' capacity to leverage their domestic private actors to act internationally, and instead view "the relationship between states and the private corporations holding the resources states seek to exploit [as] more dynamic and contested."[19][20] Acknowledging and specifying those domains where, for example, platform companies have agency (e.g., in implementing content moderation) is particularly important in light of discussions of platform companies' corporate social responsibility.[21] For example, it would be a mistake to assume full alignment between, and coordination among, platform companies, such as YouTube (owned by Google), and the US government concerning the activities of these platform companies in Russia. Conversely, it would also be wrong to disregard how both the US legal system and US public discourse shape or condition platforms' decisions under highly politicized conditions, such as the current war.

We argue that the war has had an ambiguous impact on digital authoritarianism in Russia so far. On the one hand, as Western companies leave the Russian market and Russia blocks popular Western social media platforms, the nationalization of leading digital platforms facilitates censorship, surveillance, and offline repression via *rule by law*. On the other hand, digital repressive capacities have been considerably hampered

due to the disruption of international supply chains caused by the imposition of sanctions. The future integrity of Russia's tech sector is uncertain as the lack of investment, faltering import substitution, and loss of human capital could set the sector's development back by more than a decade. Notwithstanding this ambiguity, the war has exposed the extent to which Russia's claims about achieving digital sovereignty deviate from reality, as both private and state firms have struggled to meet underfunded (and unrealistic) import substitution requirements.

The article proceeds as follows. First, we provide a brief background on the development of Russia's digital sector and the inherent tension between its efforts to integrate into the global economy and its attempts to establish digital sovereignty. Having laid out the contours of Russia's semi-dependent digital infrastructures, we analyze the shifts that have been set in motion by Russia's war against Ukraine and how these shifts affect the Russian state's capacity to control, surveil, and repress. Finally, reflect on the lessons that may be learned from the Russian case about weaponized interdependence and the significance of transnational interdependencies for understanding digital authoritarianism. **[page 23]**

Semi-dependent Digital Authoritarianism in Russia

Russia has a high internet penetration rate with 130 million users, or almost 90 percent of its population. Internationally, the country stands out for its highly developed tech sector and for the success its domestic platforms and digital services have had in outcompeting their foreign competitors. For example, among social media platforms VK (formerly known as Vkontakte) has been far more popular than Facebook. The Russian internet sector is dominated by roughly a dozen digital ecosystems, most notably VK, Sber, and Yandex. Since launching its search engine in 1997, Yandex has expanded into a wide array of services (from news aggregation to cloud hosting and the development of self-driving cars), earning it the international nickname of "Russia's answer to Google." As part of the development of its various products, Yandex has also been one of the key players in the development of algorithmic recommender systems and artificial intelligence (AI) in Russia.[22] The development of Russia's tech sector benefited from the state's initial lax approach to regulating the digital domain. Moscow actively promoted digitalization, including within the public sector, and made some progress towards implementing open government principles, as demonstrated through the state procurement portal zakupki.gov.ru.[23] Russia made significant improvements in various e-government domains, benefitting both businesses and citizens in their interactions with the state.[24]

Russia has been adept at using digital technologies and social media monitoring as feedback channels to gauge the public's preferences about policy issues and ascertain the performance of local and regional political actors.[25][26][27]

Traditional media, such as television and print, have been steadily restricted from the early 2000s onwards. In the digital domain, to the contrary, Russia had preferred to influence online discourses rather than censor online speech through internet filtering, which is in line with the notion of consultative authoritarianism.[28] This approach changed after a series of large-scale protests against election fraud in December 2011,

in which social media played an instrumental role. The government introduced website blocking soon after, and since then, it has steadily expanded a body of restrictive internet legislation.[29][30] In its efforts to censor online content, Russia has increasingly clashed with foreign platform companies and imposed increasing fines for failure to remove content.

Since 2012, Russia's digital policy has become increasingly contradictory. On the one hand, Russia has actively promoted and invested in the development of its digital economy.[31] Russian technological firms have entered foreign markets to bolster their economic position. Russia also aims to compete for a global leadership position in AI development. This push for integration into the **[page 24]** global tech economy, however, is at odds with the opposing tendency towards digital sovereignty. Driven by national security concerns, Russia has pushed for import substitution (albeit with limited success) and has made significant steps towards centralizing its control over the country's internet infrastructure to enable more effective filtering and surveillance.[32][33][34] These contradictory tendencies place a particular strain on companies that strive to expand their businesses to international markets and rely on exports for their revenue.

How the Effects of the War and Sanctions Have Enhanced Opportunities for Expanding Digital Authoritarianism

In the following two sections, we present a preliminary assessment of how Russia's war against Ukraine and the subsequent sanctions imposed upon Russia are reshaping the regime's repressive capacities. We demonstrate how the disruption of transnational digital dependencies may simultaneously enhance and undermine digital authoritarianism.

Personal and Entity Sanctions Enable Russia's Nationalization of Ownership and Concentration of Control over Domestic Digital Ecosystems

The main thrust of Western technology sanctions against Russia in the wake of the full-scale invasion of Ukraine on February 24, 2022 was aimed at undermining Russia's military-industrial complex, hampering its war effort, and inhibiting further military aggression in the medium to long term. Nonetheless, Western sanctions also directly and indirectly affected Russia's eleven major digital ecosystems, resulting in important shifts in ownership structures. The strategy to take advantage of adverse circumstances to consolidate digital technologies and services into conglomerates controlled by the state or loyal business elites builds upon previous practices. For example, in Russia, changes in ownership have been a key tool in establishing state control over online media and physical infrastructure, such as internet service providers or mobile operators.[35]

At first, digital companies closely intertwined with the current regime in Russia (via direct, majority ownership by the by the Russian state or via indirect control from oligarchs with close ties to the regime) were targeted by the sanctions. The United States targeted major state-controlled lenders Sber and VTB with blocking sanctions, and the European Union (EU) delisted them from the SWIFT payment system. Key management positions at state-controlled entities remained unaltered, except for some

international board members leaving Sber. However, personal sanctions against executives of privately-held companies— often listed on international stock exchanges—have had a profound impact on management and ownership structures. Key figures—such as Arkadii Volozh and Tigran Khudaverdian (Yandex), Aleksandr Shulgin (Ozon), and Vladimir Evtushenkov (MTS)—were urged to leave their executive positions or transfer parts of their stakes to trustees to prevent endangering their companies' busi- **[page 25]** ness operations. Nonetheless, the market shock caused losses in the billions of dollars and a decline in stock market values.

Sanctioned individuals and entities did not turn against the Kremlin, nor did they place pressure on the Russian government to halt its costly war efforts. Rather, the redistribution of company stakes and senior executive roles considerably strengthened the regime's grip on Russia's main digital ecosystems and facilitated practices of digital authoritarianism. For instance, the Dutch investment company Prosus, which had owned 100 percent of Avito (Russia's main online advertising platform) sold it to the well-connected investor and former CEO of MegaFon Ivan Tavrin in October 2022.[38]

Yandex has embarked on a painful process of disentangling its international and Russian operations, with Arkadii Volozh relocating Yandex's international business operations to Israel. In order to ensure its survival in Russia, Yandex sold its two most toxic media assets (a news aggregator called Yandex News and Yandex Zen, a content recommendation platform) to VK. The algorithms of these media assets have been directed towards promoting pro-Kremlin messages and repressing independent media.[39] The precondition of this deal was the breakup of the joint venture O2O Holding between VK and Sber. VK sold home delivery service Delivery Club to Yandex in exchange for Yandex News and Yandex Zen, the search engine's main media assets. VK's goal was to integrate these two media assets with the Yandex main webpage yandex.ru, which, at that time, was the most visited website in Russia and the eighth most popular website in the world.[40]

With this deal completed on September 12, 2022, VK consolidated its position as the main Russian digital media ecosystem with 100 million monthly users and 50 million daily users.[41] As an entirely Russian-owned digital ecosystem (headed by Vladimir Kirienko, the son of the deputy head of the Presidential Administration Sergei Kirienko) VK complies with all government regulations and requirements for internet censorship. Moreover, with its integration into the government digital services platform Gosuslugi and the obligation of state bodies to maintain their social network presence on VK, state control of Russia's main social media platform has increased considerably.[42] In November, 2022, Yandex announced that it will undergo a major restructuring to separate its Russian and international operations. The company also appointed former finance minister and head of Russia's Audit Chamber Alexei Kudrin as corporate development advisor.[43][44]

Government Response to Tech Sanctions Promotes Increased Dependence on the State

The Russian government's policy response to Western tech sanctions demonstrates awareness of the sanctions' detrimental long-term effect on Russia's digital economy, but, overall, they can be characterized as "too little, too late." Moreover, the country

has been marred by problems of bad governance that inhibit the implementation of long-term objectives. Policymakers constantly interfere with strategic goals to cater to private interests, and rent-seeking remains prevalent among the ruling elite. It has become clear that these measures will **[page 26]**

Table 1. Overview of Western Sanctions against Russia's Digital Ecosystems after Russia's Full-scale Invasion of Ukraine

Digital Ecosystem	*Main Business Activity*	*Ownership/Majority Control*	*Rank According to Market Value*	*Number of Users in Russia (in Millions, 2021)*	*Sanctioned Individuals and their Position in or Association with Company at the Time Sanctions Were Introduced*	*Countries that Imposed Sanctions on Entities*
Sber	Banking	State	1	103	German Gref (CEO); executive board	United States, European Union, United kingdom
Yandex	Search engine	Private	2	104	Tigran Khudaverdian (executive director, deputy CEO); Arkady Volozh (founder, CEO)	None
X5 Retail Group	Retail	Private	3	72.5	Mikhail Fridman (supervisory board)	None
Wildberries	E-commerce	Private	4	38.5	None	None
Tinkoff / TCS Group	Banking/Financial technology	Private	5	19	Oleg Tinkov (founder, major shareholder)	None
Ozon	E-commerce	Private	6	21.3	Aleksandr Shulgin (CEO)	None
VTB	Banking	State	7	14	Andrei Kostin (CEO); board of management	United States, European Union, United kingdom
Megafon	Mobile phone/Telecom operator	Private	8	74	Alisher Usmanov (major shareholder via his holding USM)	None
MTS	Mobile phone/Telecom operator	Private	9	79.7	Vladimir Evtushenkov (Chair of the board of Sistema, which holds a controlling stake in MTS)	None
Avito	E-commerce	Private	10	32	None	None
VK (formerly Mail.ru Group)	Social network; email	State	11	90	Vladimir Kirienko (CEO)	None

Source: Gaidar Institute and the Brookings Sanctions Tracker[36][37] **[page 27]**

further increase the nationalization of the IT sector and the role of the state therein. They are targeted at large, state-dependent entities to the detriment of the previously diverse and dynamic sector. This more proactive digital industrial policy, within a digital economy newly severed from global markets in key domains, will considerably enhance the Russian state's capacity to implement policies of digital authoritarianism.

On March 2, 2022 President Vladimir Putin published a decree on the "acceleration of development of the information technology sector." The government will support IT innovation in the framework of an annual grant system, but the allocated sum of 14 billion rubles ($136 million at that time) was too small to have a sizable effect on import substitutions. In the same vein, funding for the ongoing Digital Economy national project, launched in 2018, will be trimmed by 34 percent in the 2023 state budget.[45] The income tax rate of accredited IT companies will be slashed to zero percent until the end of 2024, and the government will provide support for cheap loans. Moreover, the government freed IT companies from tax and other state audits and currency control for the next three years. Lastly, the government offered some additional benefits to IT specialists to preempt the emigration of skilled workers, many of whom feared they would be mobilized to fight in Ukraine; military service was deferred until the age of 27, and IT workers were entitled to preferential private mortgages.[46]

The most immediate effect of this government policy was an increase in the number of Russian businesses registered as IT companies with the Ministry for Digital Development to become elligible for state benefits. By the end of August 2022, the registry officially comprised about 27,000 IT companies. However, in reality, information and communication technologies were the main business activity for less than half of these businesses. The others mainly sought registration to secure privileges. This may lead to a misallocation of up to 9 billion rubles (equivalent to $148 million in August 2022) in state funds to purposes that are only remotely related to IT.[47] Contrary to expectations raised by the March decree, the "partial" mobilization announced by Putin on September 21, 2022 demonstrated that IT professionals were not exempted from mobilization. As a result, the Ministry for Digital Development, as well as companies and business organizations, started to frantically lobby the Ministry of Defense to prevent their employees from being drafted.

In sum, neither state enterprises nor private companies turned *against* the state to lobby for ending the war. Rather, they turned *towards* the state to minimize damage and reap as many benefits as possible while the prospects of overcoming international isolation remained uncertain. **[page 28]**

Wartime Censorship Contributes to Sovereignization of the Digital Information Space

In the wake of the February 24 invasion, the Russian government employed a mix of existing instruments of internet control and new regulatory initiatives that introduced full-scale wartime censorship. In the war's first 6 months, more than 7,000 websites were blocked, and over 138,000 internet resources were either deleted or blocked. All remaining inde- pendent media, including Echo Moskvy Radio, TV Rain, and Novaya Gazeta—led by Nobel Peace laureate Dmitrii Muratov—were forced to shut down. The Russian government relied on the internet oversight body Roskomnadzor, the Prosecutor General's Office (for extra- judicial blockings), the court system, as well as

internet service providers and platform companies such as VK and Yandex to implement wartime censorship.[48]

The Russian parliament passed sixteen repressive laws, many of which introduced administrative or criminal liability for spreading information on the war at odds with official state propaganda.[49] This included "public actions aimed at discrediting the Russian army," calling for sanctions, and spreading "false information" on the Russian army or state government bodies. Moreover, the State Duma—the Rus- sian parliament's lower chamber—transferred additional powers to the Prosecutor General's Office. The Prosecutor General is now entitled to demand that Roskomnadzor withdraw the license of any domestic or foreign media firm for a broad range of deeds, including "fakes," without a court decision. "Fake" is a short- hand used in the Russian discourse to refer to the "public dissemination of knowingly false information about the use of the Armed Forces of the Russian Federation," which was introduced into law on March 4, 2022.[50] Spreading such "fakes" was turned into a criminal liability, in which one can be punished with high fines and a prison sentence of up to 15 years. The subsequent arbitrary application demonstrated that virtually any information in the public domain could be reinterpreted as "fake" if deemed politically expedient by the Russian authorities. Lastly, the Russian government tightened the administrative liability of search engines, mobile service providers, and foreign companies operating on the internet that did not implement Russian government policies nor comply with state requests to, for example, remove content or block particular accounts. As of the end of August 2022, 224 individuals have faced criminal charges in relation to the war, including 90 for allegedly spreading "fakes" and 11 for "discrediting the Russian **[page 29]** army." Furthermore, almost 4,000 Russians faced administrative charges for allegedly "discrediting the Russian army," predominantly online.[51]

In March 2022, Russia designated Meta, the parent company of Facebook and Instagram, an "extremist organization" and blocked the two platforms (though notably, the Meta-owned messaging application WhatsApp was spared from designation). Following the throttling of Twitter in 2021, platform access was fully restricted for allegedly spreading "fakes" about the war. To implement the blocking of Facebook, Instagram, and Twitter, Roskomnadzor relied on the deep packet inspection technology that internet service providers have been obliged to install since 2019 due to Russia's "sovereign internet" legislation.[52]

It was not just American companies that faced wartime censorship in Russia. In March 2022, TikTok—the short-form video service of China's ByteDance—disabled live-streaming and uploading of new video content in Russia due to the new repressive legislation on "fakes." The company aimed to safeguard its employees and users from prosecution and avoid being blocked. After the war mobilization campaign started in September 2022, TikTok allowed employees to move to Kazakhstan, Armenia, or Kyrgyzstan to evade the draft.[53] Moreover, a Russian court fined TikTok 3 million rubles ($51,000) on October 4, 2022, for failing to delete content that violates Russian laws on "LGBT propaganda," a repressive tool often used to put pressure on Russian and international entities.[54]

This wartime interference with social media had an immediate effect on active users and content on these platforms. While in May 2022 there were on average 10 percent fewer active users and 8 percent less new content, the effect was distributed among platforms. Foreign-owned social media saw a significant decrease in the number of active users after access restrictions were imposed— TikTok by 76%, Twitter by 34%, and Facebook by 33%. Although it was not blocked by Russia, YouTube also experienced a drop in its user base (15 percent), which may be related to Google's decision to suspend ad sales in Russia. This hampered content monetization and increased the likelihood that YouTube will be blocked in the near future. The remaining platforms benefited from these migrating audiences. The largest user increase occurred on Telegram (23 percent), a platform where many channels are known to have been created or co-opted by pro-Kremlin actors and whose independence from Russian authorities has been questioned.[55] Russian-owned social media VK and Odnoklassniki also gained a considerable number of active users when the state blocked foreign platforms (VK by 18% and Odnoklassniki by 4%).[56]

Roskomnadzor publicly asked social media users to switch to Russian platforms after foreign networks were banned.[57] This illustrates how the wartime censorship fits with the larger effort to nationalize the internet in Russia. Since 2021, a set of Russian applications have been required to be preinstalled on mobile phones, tablets, desktops, notebooks, and smart TVs—a move clearly targeted to crowd out international platforms.[58] Moreover, in March 2022, the Russian Ministry for Digital Development recommended that Russians exclusively use Yandex's browser to ensure uninterrupted access to all government websites, as it would no longer be guaranteed with international Transport **[page 30]** Layer Security/Secure Socket Layers (TLS/ SSL) certificates, which are important for secure https connections.[59] Due to sanctions, Western companies refused to renew certificates. Once expired, browsers reject sites with expired certificates, making an encrypted connection impossible. In response, Russia started to issue its own security certificates via the state e-government platform Gosuslugi, raising concerns about enhanced opportunities for surveilling web traffic.[60]

In sum, the Russian government's domestic wartime censorship was aimed at silencing independent media and voices on foreign and domestic platforms while incentivizing users to migrate to national platforms under full control of the Russian state. This has resulted in a greatly restricted information space, within which independent journalism and freedom of expression have been severely curtailed.

How the Effects of the War and Sanctions Exposed the Structural Constraints and Vulnerabilities of Digital Semi-Dependence

A Failed Quest for Digital Sovereignty: Export Controls, Self-sanctioning Western Companies, and Russia's Deficient Import Substitution

Since 2012, Russia's main goal in the digital domain has been to achieve digital sovereignty: full state authority over the country's internet and other digital infrastructures. At the centerpiece of Russia's understanding of this concept is information security. The Russian state aims to control the infrastructure sector in order to oversee and control the flow of data.[61] The imposition of Western sanctions after the Russian annexation of Crimea in 2014 further increased the salience of the issue. In November 2015, Russia launched a policy of import substitution with the aim of rendering the Russian state independent of foreign hardware and software. Notwithstanding its grand ambitions, on the eve of Russia's fullscale invasion of Ukraine in early 2022, Russia was far behind its declared goal of attaining digital sovereignty. In 2021, Russia imported information and communication technology (ICT) goods valued at $35.5 billion, which, according to estimates of the Higher School of Economics in Moscow, amounted to 70 percent of the added value created by the Russian ICT sector in 2021. Notably, the **[page 31]** import share in the added value of the Russian ICT sector had *grown* from 64 percent in 2019 to 67 percent in 2020, and finally 70 percent in 2021. In terms of sanctions risks, the geography of these imports is telling. While Russia imported ICT goods mainly from Asia (China 65 percent, Vietnam 8.4 percent, and Taiwan 3.7 percent), it procured computer services and software primarily from Western states (Germany 16.4 percent, US 9.6 percent, Netherlands 9.1 percent, and Cyprus 9 percent).[62]

This dependency on foreign software and licenses was particularly problematic in the public sector. In 2016, foreign-made equipment was abundant in Russian state bodies and public companies: 95 percent of web browsers, 44.5 percent of document management systems, 99.9 percent of email programs, 98 percent of communication software, 89.6 percent of office suites, and 95 percent of operating systems were foreign-made. A notable exception is antivirus programs, of which, with Russian firms such as Kaspersky, the country's share of foreign services used was 1.4 percent.[63] By the end of 2021, the share of Russian software in state companies should have been around 50–70 percent but amounted to a mere 30–35 percent. This confirms analysts' findings that Russian possibilities for import substitution in the ICT branch are limited.[64][65]

Given the faltering import substitution, the decision of over one hundred Western ICT companies to restrict their business operations in Russia had a major impact on the country's business-to-business, business-to-government, and government-to-government interactions. This self-sanctioning by Western companies affected products in information security, telecommunications equipment, servers and data storage systems, and software and licenses. Vendors differed considerably in the scale of restrictions. Some vendors halted service contracts, restricted the delivery of software and hardware, or withdrew licenses for Russian clients. Others announced the cancellation of new projects or terminated business operations in Russia

entirely.[66] According to estimates by the Russian Deputy Prime Minister Dmitrii Chernyshenko, Russia needs at least three to five years to compensate for the effect of Western vendors leaving the Russian market. In the meantime, the Russian government introduced a gray import scheme to allow the import of sanctioned goods via third countries, even without the consent of producers.[67]

Especially hard-hitting were the export controls introduced by the US, EU, and UK on microchips manufactured in the US or Europe. The world's major chip manufacturers, such as the Taiwan Semiconductor Manufacturing Company (TSMC), Intel, Samsung, Qualcomm, and ARM, were forced to comply and halt business transactions with Russia. This resulted in a powerful blow to Russia's major chip manufacturers MCST and Baikal Electronics, whose chips heavily rely on semiconductors produced by TSMC. Furthermore, **[page 32]** in mid-September, the US placed MCST and Baikal Electronics, as well as other key players of Russia's quantum computing industry, on the US Treasury Department's Specially Designated Nationals and Blocked Persons List (SDN) list. This sanction will prevent the sector from commissioning components for Russian chips from foreign firms. In a frank assessment of the domestic chip industry, the Russian Ministry for Industry and Trade admitted that Russian technologies are at least ten to fifteen years behind leading manufacturers in the world and that foreign design, components, software, and material are critical for Russian chip makers.[68][69][70] This trend is exacerbated by underinvestment in the development of AI technologies. In its AI road map until 2030 published in late 2022, the Russian government slashed investment into AI development tenfold compared to previous plans dating from 2019.[71] The deficit of state-of-the-art chips will not only hamper Russian military aggression against Ukraine but also the Russian government's maintenance and future development of digital authoritarianism at home—for example, the use of AI in social media monitoring and facial recognition technologies.

Surveillance and Filtering: The Double-edged Sword of International Dependency

In the past decade Russia has ramped up its procurement of the necessary hard- ware and software to create extensive digital surveillance capacities at home. Procurement was spearheaded by the federal government and the capital city of Moscow but also by large state-owned companies. The main goal was to automate the surveillance of citizens—both online and in major urban areas—at the expense of their personal data security and privacy. This has included the acquisition of hardware, software, and licenses to implement compulsory mass storage of user data; social media monitoring; and the development of customized applications to increase automated online censorship capacity, as well as video cameras and algorithms for a sprawling system of surveillance in urban public spaces.[72]

While the Russian government strove to rely mainly on domestic suppliers, in practice, its digital surveillance infrastructures continue to depend on foreign components and software. For instance, Moscow's sophisticated system of facial recognition has been used to track down and apprehend anti-war protesters.[73][74]

Russia's capital city surveillance relies on algorithms from four different companies, all of which are Russian-owned: NtechLab, Tevian FaceSDK, VisionLabs Luna Platform,

and Kipod (a Belarusian-Russian product).[75] This reliance on homegrown algorithms might suggest autonomy from sanction shocks. VisionLabs, owned by the MTS digital ecosystem, demonstrates that this is not the case. In order to be commercially viable, the company depends on the sale of facial recognition- **[page 33]** based payment systems to international banks. As a result of the sanctions, VisionLabs was forced to reorient the export of its products from Europe to markets in Asia, Latin America, and the Middle East.

Yet, an even bigger challenge relates to the Graphic Processing Units (GPU) required to enhance facial recognition algorithms. In March 2022, the world's leading producer of GPUs, Nvidia, which Russian companies heavily relied upon, stopped all product sales to Russia due to the war. Later in September 2022, the US government sanctioned the sale of sophisticated chips from AMD and Nvidia to Russia.[76][77] According to the founder of VisionLabs, Aleksandr Khanin, there is "currently no fully-fledged replacement for Nvidia."[78] Russia's difficulty acquiring chips from abroad, combined with a lack of funds and investment, will considerably hamper the roll-out of the ambitious "smart city" program, which leans heavily on AI and video surveillance, to Russian regions beyond Moscow.[79]

Another domain where fault lines are appearing is the mass storage of user data (including the content of users' communications) required in the framework of the so-called "Yarovaya legislation," a package of anti-terrorism measures adopted in 2016.[80] The control center of this legislation or communications surveillance system in Moscow is powered by dozens of servers from Lenovo (China) and Super Micro Computer (US). Its Deep Packet Inspection technology heavily relies on equipment provided by the Israeli company Silicom Ltd. A few months before the start of the war, Russia bought an internet traffic solution developed by IXIA, Keysight Technologies (US).[81] The entire infrastructure on which the Russian surveillance of digital communications relies demonstrates a high risk of deterioration, as these technologies can no longer be thoroughly maintained, updated, or replaced. This shows how limited

Russia's policy of import substitution was even in the domains of paramount importance to the regime, such as surveillance. It is likely that data storage and surveillance capacity will be stalled or may deteriorate until replacements for Western technology and maintenance can be procured. Due to the prohibitively high costs of servers, Russian mobile operators have lobbied the government to postpone the deadlines foreseen in the "Yarovaya legislation" for increasing storage capacity by 15 percent per year and proposed to pause the requirement for storing video content for one year.[82] **[page 34]**

As a whole, the Russian telecommunications sector will likely become more lopsided in the wake of the war. To develop Russian mobile networks, the four leading Russian operators have relied on foreign technology partners such as the European companies Nokia and Ericsson and the Chinese provider Huawei. These companies have been crucial in pushing forward the development of a Russian 5G network, as no Russian competitor currently exists. Given that Nokia and Ericsson plan to exit the Russian market by the end of 2022 and Huawei's suspension of business operations in Russia, the future of Russia's 5G network is uncertain. Russia's foreign dependence also

extends to its surveillance capacity, as Nokia has been a crucial partner in providing equipment and services to MTS for Russia's surveillance system, the System of Operative Investigative Activities (SORM).[83][84] In the early 1990s, this system was built as the Russian equivalent of the Western "lawful intercept," but gradually turned into a tool of mass surveillance for Russia's domestic intelligence, the Federal Security Service (FSB), to spy on citizens. Telecom and web companies as well as operators are obliged to install equipment that allows the FSB to circumvent courts and ISPs to monitor internet traffic directly.[85][86]

Human Capital: Brain Drain as a Major Constraint to Digital Authoritarianism

One of the major challenges facing the future development of digital authoritarianism in Russia is the loss of human capital in its IT sector. Russia has around 1.3 million IT specialists, but only 450,000 actually work in the ICT sector—those who produce software and hardware. The rest are merely employed in branches that consume digital technologies (Russia tends to label domestic sales or service companies that have robust IT departments as IT companies). In 2020, only 2.5 percent of the overall workforce was employed in IT, compared to 7.6 percent in Finland and 5.6 percent in the UK.[87]

Even before the war, human capital in Russia's IT sector was an acute problem. The Russian Ministry of Digital Development estimated that Russia lacked about 500,000 to 1,000,000 qualified IT cadres in February 2021. A survey by the Boston Consulting Group revealed that around 60 percent of programmers were willing to emigrate from Russia in late 2021.[88][89]

Russia's invasion of Ukraine exacerbated the human capital issue. Ac- cording to various assessments by IT business associations, between 40,000 and 70,000 IT professionals left Russia immediately after the outbreak of the war.[90][91] By the end of the year 2022, Russia's Minister of Digital Development Maksut Shadaev estimated 100,000 IT specialists had left Russia, likely an underestimate of the total exodus.[92] While some might have returned to Russia after the initial shock or kept working remotely for the Russian market, the cadre deficit is substantial. In a survey by the software association Russoft, almost 70 percent of respondents agreed that sanctions had impacted them directly. About 50 percent agreed that the exit of Western companies and services will slow down the development of the Russian IT sectors, while slightly more than 40 percent indicated this might also offer new chances for Russian firms. Almost 40 percent of respondents named "uneasiness, depression" as their current **[page 35]** emotional status, and 25 percent agreed there was a lack of perspective for professional development.[93]

Besides these push factors, there were also geopolitical pull factors. Countries in the region—such as Armenia, Georgia, Kazakhstan, the Baltics states — as well as Israel compete for Russian IT professionals. Armenia stated that 850 Russian companies and 50,000 Russian tech workers relocated to the country in the South Caucasus over the period between the beginning of Russia's fullscale invasion of Ukraine on February 24 and early September 2022, boosting its GDP growth forecast from 1.6 to 13 percent.[94][95] It was not only Russian and Western companies leaving Russia, such as SAP, Cisco, Oracle, Microsoft, or IBM, that were relocating their Russian IT specialists

abroad. In September, it became known that Huawei was relocating its Russian staff to Kazakhstan and Uzbekistan. In this geopolitical competition for qualified IT professionals, even Rostec, Russia's main state corporation in the military-industrial complex and a key player in AI, has struggled to fill as many as 2,500 IT vacancies per year.[96] The partial mobilization announced on September 21, 2022, led to another wave of qualified IT specialists emigrating from Russia.

In sum, this dearth of qualified IT professionals poses a serious challenge for Russia to maintain its ability to advance digital authoritarianism domestically. It may also markedly reduce Russian capacities as both the tech sector and surveillance authorities, such as Roskomnadzor, rely on highly skilled employees.

Russia's Tech Dependency on China Is Growing Despite Limits of the Sino-Russian Partnership

In the past, Russia has demonstrated an aversion to becoming too dependent on Chinese technologies. The government has harbored a great deal of distrust towards Chinese infrastructure such as 5G technology due to associated security risks. As such, it has refrained from buying security and surveillance technology exclusively from China.[97] While Russia and China have built a high-tech partnership over time, it is a complex relationship fraught with many problems.[98] In 2021, China accounted for 70 percent of Russia's technology imports, such as computers, semiconductors, and telecom equipment.[99] With major US and European companies leaving the Russian market in 2022, US tech sanctions in place, and the Russian import substitution program not living up to its promises, a further turn to China at one time appeared likely.

But at the time of writing, it has become clear that there is neither the capacity nor the willingness to deepen the bilateral tech partnership "without limits." China is mainly looking out for its economic interests and is hedging its bets to try to avoid the imposition of secondary sanctions on its tech companies. Huawei, for example, not only relocated employees from Russia to Kazakhstan and Uzbekistan, but it also stopped deliveries and sales of new products at its official retail stores and in its online shops in Russia. In a similar vein, China's Lenovo and Xiaomi have curtailed deliveries of consumer electronics to Russia due to their dependency on US chips in their supply chain. Furthermore, the departure of major Western logistics companies from the Russian market have **[page 36]** created significant logistical disruptions. Since February, the price for container deliveries from China to Russia has almost doubled, leading to a surge in prices of the respective electronics produced by Chinese companies still operating in Russia.[100]

Even if China had wanted to consolidate its role as Russia's main partner for high-end technologies, it would face substantial obstacles in doing so. China's chip sector lags several generations behind world leaders, such as Taiwan's TSMC, which halted deliveries to Russia in the wake of the war. Moreover, Chinese chipmakers heavily rely on US high-end components in their supply chain, which makes them vulnerable to US sanction pressures. Therefore, at least concerning modern chips, no immediate mutually beneficial Sino-Russian convergence is in sight.[101][102][103]

Servers and data centers have become key technology items that Russia is increasingly dependent on. In July, it became known that Russia's Ministry of Internal Affairs has plans to spend almost 1 billion rubles ($18 million) on Huawei servers for its new data center in Moscow, which is set to be completed by 2024.[104] Similarly, in September, Russia's major state-owned bank Sber published a tender of $130 million on servers with characteristics that only Chinese producers, such as Lenovo and Huawei, can meet.[105] Both the MIA and Sber rejected servers with Russian-made Elbrus components due to concerns about quality and compatibility, even though the Russian government prescribes Russian-made technology for critical infrastructure. Whether Chinese firms can deliver on these tenders is currently uncertain.

While both Russian government officials and key private companies in the digital economy have been wary of security-related issues concerning Chinese products, as well as potential overreliance on a single geopolitical powerhouse, Russia's international isolation will push it to lean more heavily on Chinese tech products.

Conclusion

This article aimed to examine how authoritarian states' dependence on foreign digital technologies and services shapes and constrains their capacity to control, surveil, and repress domestically. To illustrate the core argument that globalized digital infrastructures matter in understanding digital authoritarianism, the article examined how Russia's war against Ukraine, and the sanctions imposed on Russia in response, have influenced its domestic repressive capacities. When examining February-September 2022, we found that the war has had an ambiguous effect, both providing enhanced capacity for digital authoritarianism (e.g., through nationalization) and undermining the future integrity of the digital infrastructures on which this repressive apparatus relies. We also demonstrated how the resulting geopolitical shift has belied previous expectations, as China turned out to be reluctant and, to some extent, unable to fill the void left by the departure of Western tech firms from Russia. **[page 37]**

The events that have unfolded in Russia demonstrate how capacity and performance in digital authoritarianism are dependent on the stability and integrity of digital infrastructures. Notwithstanding claims about digital sovereignty and import substitution, these infra- structures are transnationally dependent in ways that may undermine autocrats' capacity to use digital technologies to their advantage. It also shows the extent of disruption tech sanctions may cause. "Weaponizing" interdependence in the domain of digital infrastructures can thus inflict major damage. At the same time, the Russian case also illustrates how "weaponizing" interdependence in this way can result in a fundamental recalibration in both markets and the configuration of the digital infrastructures themselves. As it sets in motion these processes of adjustment, the interdependency that was weaponized may in whole or in part cease to exist, precluding a state from exerting such influence on a future occasion.

Notes

[1] Manuel Castells, Networks of Outrage and Hope: Social Movements in the Internet Age (Cambridge, UK and Malden, MA: Polity Press, 2015): 246–271.

[2] Hillary Rodham Clinton, “Remarks on Internet Freedom,” U.S. Department of State, January 21, 2010,https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[3] Larry Diamond, “Liberation Technology,” Journal of Democracy 21, no. 3 (2010): 69–83, doi:10.1353/jod.0.0190.

[4] Rebecca MacKinnon, “Liberation Technology: China’s ‘Networked Authoritarianism,’” Journal of Democracy 22, no. 2 (2011): 33, doi:10.1353/jod.2011.0033.

[5] Eda Keremoğlu and Nils B. Weidmann, “How Dictators Control the Internet: A Review Essay,” Comparative Political Studies 53, no. 10–11 (2020): 1690–1703, https://doi.org/10.1177/0010414020912278.

[6] Seva Gunitsky, “Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability,” Perspectives on Politics 13, no. 1 (2015): 42–54, https://doi.org/10.1017/S1537592714003120.

[7] 7 Ibid.

[8] Sebastian Stier, “Internet Diffusion and Regime Type: Temporal Patterns in Technology Adoption,” Telecommunications Policy 41, no. 1 (2017): 25–34, https://doi.org/10.1016/j.telpol.2016.10.005.

[9] Sergei Guriev and Daniel Treisman, “A Theory of Informational Autocracy,” Journal of Public Economics 186 (2020): 1, https://doi.org/10.1016/j.jpubeco.2020.104158.

[10] Seva Gunitsky, “Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability,” Perspectives on Politics 13, no. 1 (2015): 42–54, https://doi.org/10.1017/S1537592714003120.

[11] Eda Keremoğlu and Nils B. Weidmann, “How Dictators Control the Internet: A Review Essay,” Comparative Political Studies 53, no. 10–11 (2020): 1690–1703, https://doi.org/10.1177/0010414020912278.

[12] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, “The Digital Dictators,” Foreign Affairs 99, no. 1 (2020): 103–115, https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

[13] Nils B. Weidmann and Espen Geelmuyden Rød, The Internet and Political Protest in Autocracies, Oxford Studies in Digital Politics (Oxford, New York: Oxford University Press, 2019): 77–142. **[page 38]**

[14] Georg Glasze et al., “Contested Spatialities of Digital Sovereignty,” Geopolitics (2022): 1–40, https://doi.org/10.1080/14650045.2022.2050070.

[15] Julia Pohle and Thorsten Thiel, “Digital Sovereignty,” Internet Policy Review 9, no. 4 (2020): 1–19, https://doi.org/10.14763/2020.4.1532.

[16] Tina Freyburg and Lisa Garbe, “Authoritarian Practices in the Digital Age Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa,” International Journal of Communication 12 (2018): 3896-3916, https://ijoc.org/index.php/ijoc/article/view/8546.

[17] Henry Farrell and Abraham L. Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” International Security 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351.
[18] Abraham Newman, The Uses and Abuses of Weaponized Interdependence (Washington, D.C.: Brookings Institution Press, 2021): 55.
[19] Lars Gjesvik, “Private Infrastructure in Weaponized Interdependence,” Review of International Political Economy (2022): 1–25, https://doi.org/10.1080/09692290.2022.2069145.
[20] Laura DeNardis, The Global War for Internet Governance (New Haven: Yale University Press, 2014): 11.
[21] Mariëlle Wijermars and Tetyana Lokot, “Is Telegram a ‘Harbinger of Freedom’? The Performance, Practices, and Perception of Platforms as Political Actors in Authoritarian States,” Post-Soviet Affairs 38, no. 1–2 (2022): 125–45, https://doi.org/10.1080/1060586X.2022.2030645.
[22] Mykola Makhortykh and Mariëlle Wijermars, “Can Filter Bubbles Protect Information Freedom? Discussions of Algorithmic News Recommenders in Eastern Europe,” Digital Journalism, (2021): 1–25, https://doi.org/10.1080/21670811.2021.1970601.
[23] Mariëlle Wijermars, “The Digitalization of Russian Politics and Political Participation,” in The Palgrave Handbook of Digital Russia Studies, ed. Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Springer International Publishing, 2021): 15–32.
[24] Daria Gritsenko and Mikhail Zherebtsov, “E-Government in Russia: Plans, Reality, and Future Outlook,” in The Palgrave Handbook of Digital Russia Studies, ed. Daria Gritsenko, Mariëlle Wijermars, and Mikhail Kopotev (Cham: Springer International Publishing, 2021): 33–51.
[25] Nisan Gorgulu, Gulnaz Sharafutdinova, and Jevgenijs Steinbuks, “Political Dividends of Digital Participatory Governance: Evidence from Moscow Pothole Management,” Policy Research Working Paper Series (Washington, DC: World Bank, October 20, 2020), https://openknowledge.worldbank.org/bitstream/handle/10986/34653/Political-Dividends-of-Digital-ParticipatoryGovernance-Evidence-from-Moscow-Pothole-Management.pdf?sequence=1.
[26] Daria Gritsenko and Andrey Indukaev, “Digitalizing City Governance in Russia: The Case of the ‘Active Citizen’ Platform,” Europe-Asia Studies 73, no. 6 (2021): 1102–1124, https://doi.org/10.1080/09668136.2021.1946013.
[27] Caroline Schlaufer, “Why Do Nondemocratic Regimes Promote E-Participation? The Case of Moscow’s Active Citizen Online Voting Platform,” Governance 34, no. 3 (2021): 821–36, https://doi.org/10.1111/gove.12531.
[28] Florian Toepfl, “Innovating Consultative Authoritarianism: Internet Votes as a Novel Digital Tool to Stabilize Non-Democratic Rule in Russia,” New Media & Society 20, no. 3 (2018): 956–972, https://doi.org/10.1177/1461444816675444.
[29] Ronald Deibert et al., ed., Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (Cambridge, MA: MIT Press, 2010): 209–220.

[30] Liudmila Sivetc, “The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges,” in Freedom of Expression in Russia’s New Mediasphere, ed. Mariëlle Wijermars and Katja Lehtisaari (Routledge, 2020): 39–56.
[31] World Bank Group, “Competing in the Digital Age: Policy Implications for the Russian Federation” (Washington, DC: World Bank, 2018), https://www.worldbank.org/en/country/russia/publication/competing-in-digital-age.
[32] Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani, “A Market of Black Boxes: The Political Economy of Internet Surveillance and Censorship in Russia,” Journal of Information Technology & Politics 19, no. 1 (2022): 18–33, https://doi.org/10.1080/19331681.2021.1905972. **[page 39]**
[33] Julien Nocetti, “Russia’s ‘Dictatorship-of-the-Law’ Approach to Internet Policy,” Internet Policy Review 4, no. 4 (2015): 1–19, https://policyreview.info/articles/analysis/russias-dictatorship-law-approach-internet-policy.
[34] Ilona Stadnik, “Control by Infrastructure: Political Ambitions Meet Technical Implementations in RuNet,” First Monday 26, no. 5 (2021), https://doi.org/10.5210/fm.v26i5.11693.
[35] Carolina Vendil Pallin, “Internet Control through Ownership: The Case of Russia,” Post-Soviet Affairs 33, no. 1 (2017): 16–33, https://doi.org/10.1080/1060586X.2015.1121712.
[36] Gaidar Institute, “Цифровые экосистемы в России: эволюция, типология, подходы к регулированию [Digital Ecosystems in Russia: Evolution, Typology, Approaches to Regulation],” (Moscow: Gaidar Institute, 2022), https://www.iep.ru/files/news/Issledovanie_jekosistem_Otchet.pdf.
[37] Norman Eisen et al., “The Brookings Sanctions Tracker,” The Brookings Institution, September 14, 2022, https://www.brookings.edu/research/the-brookings-sanctions-tracker/.
[38] Valeriia Pozychaniuk and Petr Mironenko, “Как и зачем Иван Таврин купил Avito [How and Why Ivan Tavrin Bought Avito],” The Bell, October 17, 2022, https://thebell.io/novyj-vladelets-avito-vse-sposoby-pokupki-kripty-v-rossii-i-reklamnyj-spisok-roskomnadzora.
[39] Olga Dovbysh, Mariëlle Wijermars, and Mykola Makhortykh, “How to Reach Nirvana: Yandex, News Personalisation, and the Future of Russian Journalistic Media,” Digital Journalism (2022): 1–20, https://doi.org/10.1080/21670811.2021.2024080.
[40] Valeriia Pozychaniuk, “Как «Яндекс» обменял свою главную страницу в сделке с VK [How ‘Yandex’ Swapped Its Homepage in the Deal with VK],” The Bell, October 28, 2022, https://thebell.io/kak-yandeks-rasstalsya-s-glavnoy-stranitsey-runeta-donosy-ot-polzovateley-i-novyy-skandal-vokrug-twitter.
[41] Yandex Press Service, “Яндекс закрыл сделку по продаже Дзена и Новостей и покупке Delivery Club [Yandex Closed the Deal to Sell Zen and News and Buy Delivery Club],” Yandex, September 12, 2022, https://yandex.ru/company/press_releases/2022/12-09-2022.

[42] Valeriia Pozychaniuk, “Как VK пытается стать сервисом, без которого невозможно обойтись [How VK Wants to Become an Indispensable Service],” The Bell, July 10, 2022, https://thebell.io/kak-vk-skupaet-aktivy-novaya-kriptotragediya-i-razvod-twitter-c-maskom.
[43] Yandex Press Service, “Yandex N.V. Provides Strategic Update on Potential Changes to the Group’s Corporate Structure,” Yandex, November 25, 2022, https://yandex.com/company/press_center/press_releases/2022/2022-11-25.
[44] “Alexey Kudrin Joins Yandex as Part of Reorganization Plan,” Meduza, December 5, 2022, https://meduza.io/en/news/2022/12/05/alexey-kudrin-joins-yandex-as-part-of-reorganization-plan.
[45] “Бюджет нацпрограммы ‘Цифровая экономика’ в 2023 году предложено сократить на 35% [The Budget of the National Program ‘Digital Economy’ for the Year 2023 is Proposed to Be Cut by 35%],” Interfax, September 28, 2022, https://www.interfax.ru/business/865340.
[46] Vladimir Putin, “Указ о Мерах По Обеспечению Ускоренного Развития Отрасли Информационных Технологий в России [Decree on Measures to Provide for the Acceleration of the Development of Information Technologies in Russia],” Kremlin.ru, March 2, 2022, http://kremlin.ru/events/president/news/67893.
[47] “Утро софтверной казни. Реестр российских IT-компаний ждет еще одна чистка [The Morning of Software Execution. The Registry of Russian IT Companies Is About to Undergo Another Purge],” Kommersant, August 15, 2022, https://www.kommersant.ru/doc/5513074.
[48] “За Полгода Военной Цензуры Под Блокировку Попали Около 7 Тысяч Интернет-Ресурсов. Большой Обзор [Half a Year of War Censorhip: Approximately Seven Thousand Internet Resources Have Been Blocked. A Detailed Overview],” Roskomsvoboda, August 23, 2022, https://roskomsvoboda.org/post/polgoda-voyennoi-cenzury/.
[49] “Summary of Anti-War Repressions. Six Months of War,” OVD-Info, August 17, 2022, https://en.ovdinfo.org/summary-anti-war-repressions-six-months-war#1.
[50] 50 Ibid.
[51] 51 Ibid.
[52] Ilona Stadnik, “Control by Infrastructure: Political Ambitions Meet Technical Implementations in RuNet,” First Monday (2021), https://doi.org/10.5210/fm.v26i5.11693. **[page 40]**
[53] “RBC: TikTok offered to let Russian employees move abroad to evade the draft.” Meduza, November 1, 2022, https://meduza.io/en/news/2022/11/01/rbk-tiktok-offered-to-let-russian-employees-move-abroad-to-evade-the-draft.
[54] Alexander Marrow, “Russia fines TikTok for ‘LGBT propaganda’, Twitch over Ukraine content,” Reuters, October 4, 2022, https://www.reuters.com/technology/russian-court-fines-tiktok-50000-over-refusal-delete-lgbt-content-2022-10-04/.
[55] Wijermars and Lokot, “Is Telegram a ‘Harbinger of Freedom’?,” Post-Soviet Affairs (2022): 125-145, https://doi.org/10.1080/1060586X.2022.2030645.

[56] Vasilii Chernyi, “Несмотря На Блокировки, Число Авторов в Соцсетях Снизилось Лишь На 10% [The Number of Authors on Social Media Has Only Declined by 10 Percent despite Blocking],” Brand Analytics, May 21, 2022, https://br-analytics.ru/blog/changing-social-networks/.
[57] Ministry of Digital Development, “TLS-сертификаты доступны для установки на смартфоны, компьютеры и планшеты [TLS Certificates Are Available for Installation on Smartphones, Computers, and Tablets],” September 19, 2022, https://digital.gov.ru/ru/events/41990/.
[58] 58 Ibid.
[59] 59 Ibid.
[60] 60 Ibid.
[61] Anna Litvinenko, “Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty,” Media and Communication 9, no. 4 (2021): 5-15, https://doi.org/10.17645/mac.v9i4.4292.
[62] Higher School of Economics, “Цифровая Трансформация: Ожидания и Реальность: Доклад НИУ ВШЭ [Digital Transformation: Expectations and Reality: Report of the National Research University Higher School of Economics],” (Moscow: National Research University Higher School of Economics, 2022), 23-24, https://publications.hse.ru/books/617690103.
[63] Ilia Massukh, “О Состоянии Импортозамещения Прикладного Программного Обеспечения в Российской Федерации [On the State of Import Substitution of Application Software in the Russian Federation]” (Moscow: Competence Center for Import Substitution in the Sphere of Information and Communication Technologies, 2017), https://tinyurl.com/mryp4m2z.
[64] Alena Epifanova and Philipp Dietrich, “Russia’s Quest for Digital Sovereignty. Ambitions, Realities, and Its Place in the World,” DGAP Analysis (Berlin: German Council on Foreign Relations (DGAP), February 21, 2022), https://dgap.org/en/research/publications/russias-quest-digital-sovereignty.
[65] Heli Simola, “Made in Russia? Assessing Russia’s Potential for Import Substitution,” BOFIT Policy Brief (Bank of Finland Institute for Emerging Economies, 2022), https://helda.helsinki.fi/bof/handle/123456789/18404
[66] Andrei Nikitin, “Санкции в Сфере Информационных Технологий: Последствия и Риски [Sanctions in the Sphere of Information Technologies: Consequences and Risks]” (Moscow: Institute of World Economy and International Relations, April 6, 2022), https://www.imemo.ru/publications/relevant-comments/text/sanctions-in-the-field-of-information-technologyconsequences-and-risks.
[67] “Потенциал IT-отрасли в РФ может за 3-5 лет компенсировать последствия от санкций – Чернышенко [The Russian IT Sector Can Compensate for the Impact of Sanctions within Three to Five Years—Chernyshenko],” Interfax, July 18, 2022, https://www.interfax-russia.ru/moscow/news/potencial-it-otrasli-v-rf-mozhet-za-3-5-let-kompensirovat-posledstviya-ot-sankciy-chernyshenko.

[68] Anna Gross and Max Seddon, "'Everything is gone': Russian business hit hard by tech sanctions," Financial Times, June 2, 2022, https://www.ft.com/content/caf2cd3c-1f42-4e4a-b24b-c0ed803a6245.
[69] U.S. Department of the Treasury, "Russia-related Designations," Department of the Treasury's Office of Foreign Assets Control (OFAC), September 15, 2022, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220915.
[70] Nikita Korolev, "Электронику начнут с чистого нуля. Подготовлена стратегия развития отрасли до 2030 года [Electronics will start from scratch. A strategy for industry development until 2030 has been prepared]," Kommersant, September 13, 2022, https://www.kommersant.ru/doc/5558844. **[page 41]**
[71] Nikita Korolev, "Искусственный интеллект пошел на убыль. Власти скорректировали планы развития технологий [Artificial intelligence has gone downhill. The Russian government has adjusted technology development plans]," Kommersant, January 18, 2023, https://www.kommersant.ru/doc/5773647.
[72] Evgenii Kravchenko et al., "Государственный Шоппинг. Мониторинг Госзакупок: Что Покупают, Чтобы Следить За Нами [State Shopping. Monitoring of State Procurement: What They Buy to Surveil Us]," (Roskomsvoboda, December 24, 2021): 6-19, https://roskomsvoboda.org/uploads/gosud_shoping.pdf.
[73] "How Authorities Use Cameras and Facial Recognition against Protesters" OVD-Info, January 17, 2022, https://en.ovdinfo.org/how-authorities-use-cameras-and-facial-recognition-against-protesters.
[74] Сетевые Свободы [Net Freedoms Project] (@NFP_Hotline), "Технологии Политического Профайлинга [Technologies of Political Profiling]," Telegram, August 25, 2022, https://t.me/NetFreedomsProject/609.
[75] Andrei Zakharov, "Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам [Anger, Fear and Silhouettes. Moscow Mayor's Office Revealed What Algorithms Are Used for Facial Recognition]," BBC Russian Service, August 25, 2022, https://www.bbc.com/russian/features-62658404.
[76] Michael Kan, "Nvidia: We're Ceasing All Business Activities in Russia," PCMag, October 4, 2022, https://www.pcmag.com/news/nvidia-were-ceasing-all-business-activities-in-russia.
[77] Don Clark and Ana Swanson, "U.S. Restricts Sales of Sophisticated Chips to China and Russia," The New York Times, August 31, 2022, https://www.nytimes.com/2022/08/31/technology/gpu-chips-china-russia.html.
[78] "Основатель VisionLabs — РБК: «Замены картам Nvidia нет, это наша боль» [Founder of VisionLabs to RBC: There Is Not Replacement for Nvidia Chips, This Is Our Pain]," RBC, August 26, 2022, https://www.rbc.ru/newspaper/2022/08/26/62fb93289a79475e2125545f.
[79] Máté S. Csukás and Roland Z. Szabó, "The Many Faces of the Smart City: Differing Value Propositions in the Activity of Portfolios of Nine Cities," Cities 112 (2021): 103-116, https://doi.org/10.1016/j.cities.2021.103116.

[80] Liudmila Sivetc, “Controlling Free Expression ‘by Infrastructure’ in the Russian Internet: The Consequences of RuNet Sovereignization,” First Monday 26, no. 5 (2021), https://doi.org/10.5210/fm.v26i5.11698.
[81] Andrei Soldatov and Irina Borogan, “How Western Tech Companies Are Helping Russia Censor the Internet,” Washington Post, December 21, 2021, https://www.washingtonpost.com/opinions/2021/12/21/how-western-tech-companies-are-helping-russia-censor-internet/.
[82] “Власти требуют от сотовых операторов запретить безлимитные тарифы на интернет [Authorities Require Mobile Operators to Ban Unlimited Internet Tariffs],” Cnews, March 29, 2022, https://www.cnews.ru/news/top/2022-03-29_vlasti_trebuyut_ot_sotovyh.
[83] Adam Satariano, Paul Mozur, and Aaron Krolik, “When Nokia Pulled Out of Russia, a Vast Surveillance System Remained,” The New York Times, March 28, 2022, https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html.
[84] “Telecommunications Breakdown: How Russian Telco Infrastructure Was Exposed,” UpGuard, September 18, 2019, https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure.
[85] Adam Satariano et al., “When Nokia Pulled Out of Russia, a Vast Surveillance System Remained,” The New York Times, March 28, 2022, https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html.
[86] “Telecommunications Breakdown: How Russian Telco Infrastructure Was Exposed,” UpGuard, September 18, 2019, https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure.
[87] Institute for Statistical Research and Economic Knowledge, “Цифровая Экономика 2022: Краткий Статистический Сборник [Digital Economy 2022: A Brief Statistical Compendium]” (Moscow: National Research University Higher School of Economics, 2022), https://publications.hse.ru/books/553808522.
[88] El’ias Kasmi, “Две трети ИТ-специалистов готовы бежать из России [Two-thirds of IT specialists are ready to leave Russia],” CNews, November 30, 2021, https://www.cnews.ru/news/top/2021-11-30_rossiya_mozhet_ostatsya_bez.
[page 42]
[89] “Дефицит ИТ-мозгов: как Россия решает проблему кадрового голода в отрасли [A Deficit of Brains in IT: How Russia is Solving the Problem of Staff Shortage in the Industry],” RBC, July 28, 2022, https://www.rbc.ru/economics/28/07/2022/62e12c929a794747597da279.
[90] Timofei Kornev and Ekaterina Iasakova, “Эксперты оценили отток ИТ-специалистов к концу первого полугодия [Experts estimated the outflow of IT specialists’ by the end of the first half of the year],” RBC, May 28, 2022, https://www.rbc.ru/technology_and_media/28/05/2022/628fa85d9a7947dabe3b3e30.

[91] “Глава РАЭК сообщил об отъезде до 70 тыс. айтишников из России [RAEC head estimated that up to 70 thousand IT-specialists left Russia],” Kommersant, March 22, 2022, https://www.kommersant.ru/doc/5270879.
[92] Ian Martyniuk, “Код на исходе. Россию мог покинуть каждый четвертый активный ITразработчик, показывают открытые данные [The code is running out. One in four active IT developers could have left Russia, open data shows],” Novaya Gazeta Evropy, January 11, 2023, https://novayagazeta.eu/articles/2023/01/11/kod-na-iskhode.
[93] “Результаты Интернет Исследований По Теме: «ИТ-Специалисты» [Results of the Online Surveys ‘IT Specialists’],” (Russoft, April 11, 2022), https://russoft.org/wp-content/uploads/2022/04/Prezentatsiya-issledovaniya-18.04.pdf.
[94] Армения приняла свыше 50 тысяч IT-специалистов из России [More than 50,000 IT Specialists from Russia Relocated to Armenia],” Rtvi, September 5, 2022, https://rtvi.com/news/armeniya-prinyala-svyshe-50-tysyach-it-speczialistov-iz-rossii/.
[95] “Глава ЦБ Армении объяснил пересмотр прогноза роста ВВП на 2022 год с 1,6% до 13% [The Chairman of Armenia’s Central Bank Explained the Revision of Its GDP Growth Forecast for 2022 from 1.6% to 13%],” Arka News Agency, October 18, 2022, http://arka.am/ru/news/economy/glava_tsb_armenii_obyasnil_peresmotr_prognoza_rosta_vvp_na_2022_god_s_1_6_do_13/.
[96] “«Ростех»: в России серьезный дефицит ИТ-кадров [Rostec: Russia Has a Serious Shortage of IT Personnel],” Cnews, August 24, 2022, https://www.cnews.ru/news/top/2022-08-24_v_rostehe_sereznyj_defitsit.
[97] Andrei Kolesnikov and Leonid Kovachich, “Digital Authoritarianism with Russian Characteristics?” Carnegie Endowment for International Peace, April 21, 2021, https://carnegiemoscow.org/2021/04/21/digital-authoritarianism-with-russian-characteristics-pub-84346.
[98] Elsa Kania and Samuel Bendett, “A New Sino-Russian High-Tech Partnership. Authoritarian Innovation in an Era of Great-Power Rivalry,” (Australian Strategic Policy Institute, October 29, 2019), http://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.
[99] Karen M. Sutter and Michael D. Sutherland, “China’s Economic and Trade Ties with Russia,” CRS Report (Washington, DC: Congressional Research Service), https://crsreports.congress.gov/product/pdf/IF/IF12120.
[100] “Электроника дорожает в дороге. Цены на поставки из Китая и Турции удвоились [Electronics Are Getting More Expensive. Prices for Shipments from China and Turkey Have Doubled],” Kommersant, August 29, 2022, https://www.kommersant.ru/doc/5535403.
[101] Chris Miller, Chip war: the fight for the world’s most critical technology (New York: Scribner, an imprint of Simon & Schuster, 2022): 286-287.
[102] Sophie-Charlotte Fischer, “The China Factor in Tech Export Controls Against Russia,” The Diplomat, March 8, 2022, https://thediplomat.com/2022/03/the-china-factor-in-tech-export-controls-against-russia/.

[103] Maria Shagina and Emily Kilcrease, “Can Russia Rebuild Its Tech Sector with China’s Help?,” War on the Rocks, June 2, 2022, https://warontherocks.com/2022/06/can-russia-rebuild-its-tech-sector-with-chinas-help/.

[104] “МВД за миллиард ищет серверы по 5,5 млн руб. за штуку [The Ministry of Internal Affairs Is Looking for Servers for a Billion Rubles in Total, at 5.5 Million Rubles Apiece],” Cnews, July 20, 2022, https://www.cnews.ru/news/top/2022-07-20_mvd_ishchet_dve_sotni_serverov.

[105] “«Сбер» выбрал китайских производителей серверов вместо отечественных [Sber Selected Chinese Server Manufacturers Instead of Domestic Ones],” RBC, September 15, 2022, https://www.rbc.ru/technology_and_media/15/09/2022/6321fa8f9a794714af55d0e9. **[page 43]**