No. 298 18 July 2023

www.css.ethz.ch/en/publications/rad.html

RUSSIA'S TECHNOLOGICAL SOVEREIGNTY

German Association for
East European Studies

Institute for European,
Russian, and Eurasian Studies
The George Washington
University

Research Centre
for East European Studies
University of Bremen

Center for
Security Studies
ETH Zurich

Center for
Eastern European Studies
University of Zurich

ANALYSIS

Sanctions Calling: The Dire Prospects for Russia's Chips Industry

Julien Nocetti (French Institute for International Relations (IFRI), Paris)

DOI: 10.3929/ethz-b-000621535

Abstract

Integrated circuits, or semiconductors, are dual-use technologies that have a wide variety of applications, from smartphones to missile systems. Successive global crises—Sino-U.S. competition, the Covid pandemic, the war in Ukraine—have highlighted their strategic nature. When it comes to Russia, the country's already fragile position when it comes to hardware has been intensifying due to international sanctions that particularly target the national semiconductor industry. Technological sovereignty through "indigenization" of the semiconductor industry seems highly unlikely, and the defense sector—as an avid consumer of chips—will particularly suffer from sanctions.

Hardware Weaknesses: The Russian Semiconductor Industry and Market

Russia's domestic semiconductor production is many years behind the industry standard in the West. Following the breakup of the Soviet Union, the domestic electronic component industry, which largely supplied the defense, space, and nuclear industries, saw its production nosedive (Dzhalilov and Pivovarov 2017).

The proportion of electronic equipment produced and consumed in Russia domestically declined to approximately 12 percent; for comparison, in OECD countries, domestic production meets, on average, 70–80 percent of domestic needs (Borisov 2016). The 2000s saw Russia fall even further behind the US and China: by 2016, 80 percent of IT in Russia was reportedly imported (Tolkachev and Teplyakov 2018), reinforcing the idea that Russia had missed out on a revolution in those fields. Russia accounted for just 0.44 percent of global production of chips in 2009; its share increased only slowly thereafter, never surpassing 3 percent in the 2010s and falling again after 2014 and the West's imposition of sanctions (Volostnov 2019). In 2013, the Vice President of the Russian Union of Engineers described the national electronics industry as being "in a state of advanced obsolescence." Russia's leaders subsequently began to address the problem: in 2016, Putin set the goal of increasing Russian production of sophisticated civil and dual-use electronic components (Putin 2016). Nevertheless, as of 2018, these still accounted for just 27 percent of Russian consumption (Volostnov 2019).

Two years later, and with the technological competition between China and the United States having intensified, advanced semiconductors became part of a movement within Russia to catch up technologically and to make the sector "sovereign." Producing its own components came to be understood as one of the prerequisites for the country's digital sovereignty (Bezrukov 2017).

In January 2020, the new Prime Minister, Mikhail Mishustin, oversaw the approval of the "Strategy for the Development of the Russian Electronics Industry until 2030" (Government of the Russian Federation 2020). The strategy sets out three stages: a first phase of import-substitution, followed by a phase of promoting Russian technology on international markets, and finally an attempt to achieve technological preeminence. This highly ambitious strategy exemplifies the global trend toward protectionism in technology, which flies in the face of geo-economic constraints such as the destabilization of supply chains, as well as technological ones such as the miniaturization of ever-more-sophisticated chips.

Like China, Russia's problem is less having a workforce with the appropriate skills and more its ability to build the necessary ecosystem and supply chains for semiconductors. Nevertheless, some moves from 2019 point to a proactive approach, such as the private Russian firm Yadro's purchase of a controlling stake in the Russian company Syntacore. Syntacore is the founder of an international consortium that is developing an open-source processor architecture (RISC-V) designed to rival world leaders such as Intel.

The two main domestic producers—Baikal Electronics and MCST—both suffer from weaknesses: the former cannot rely on Russian solutions, as it manufactures processors based on the architecture of the British-born company ARM, while the latter does not develop products suitable for the mass market. Both domestic actors were dependent on Taiwan Semiconductor Manufacturing Company's (TSMC) production facilities before sanctions against Russia were introduced.

Chips and Sanctions: Impact on Russian Imports

In a quick and coordinated move following the onset of Russia's full-scale military aggression against Ukraine, Western countries have adopted a series of measures designed to cut off Russia from the main global technological supply chains. These have taken several forms, first and foremost controls on Western exports of certain technologies, in particular dual ones (i.e., those that have both civilian and military applications). The measures target, in particular, Russia's access to Western semiconductors.

Knowing that Russia needed this technology for its war efforts, the United States and its European and Asian allies targeted semiconductor exports early on by imposing export control measures. Following the imposition of these controls and the exit of multinational firms from the Russian market, Russian imports of integrated circuits declined significantly. Imports remain much lower than pre-invasion levels. However, Russia has made significant efforts to establish a network of suppliers in non-sanctioning countries from which to source semiconductors for potential use in military applications.

Russia thus continues to be able to source a range of integrated circuits, albeit at a much lower volume than before the war. These come primarily from China and Hong Kong (Global Trade Tracker Database 2023), which amounted in November 2022 to 55 percent of median prewar exports to Russia from all countries. (November 2022 exports from China and Hong Kong were 45 percent of 2019 imports and 33 percent of 2021 imports, respectively.) There was a report, however, of high failure rates for semiconductors from China.

According to some reports, global exports to Russia in 2022 included goods produced by major multinational manufacturers that were shipped by third parties ("Russian Import Network…" 2023). They also included exports to Russian firms that supplied the military. The main types of integrated circuits exported to Russia by Hong Kong and China since the invasion of Ukraine have been processors and controllers (Global Trade Tracker Database 2023).

As with other goods, a small volume is also transshipped through other countries.

The Sanctions' Effect on Chips: Primarily Pressuring the Russian Defense Industry?

The weaknesses of Russia's domestic industry make Russian weapons, communications, and electronic warfare systems highly reliant on Western-manufactured microchips, which are currently restricted under the allied export regulations (Manners 2022). For instance, according to the UK-based Royal United Services Institute (RUSI), the Orlan-10 UAV contains U.S.-made chips manufactured by Texas Instruments and Honeywell (Byrne et al. 2022). Furthermore, an investigation by Conflict Armament Research has shown that satellite navigation units in several Russian missiles—such as the 3M14, 9M544, Kh-59, and Kh-101—contain multiple foreign-made micro-components manufactured between 2012 and 2020 (Conflict Armament Research 2022). The Russian Iskandr and Kalibr missile systems are teeming with cutting-edge semiconductors that integrate Western technologies (Byrne 2022).

Russia's newly developed radio communications systems—including the Azart portable radio station, designed to provide jamming and secure communications at the tactical level—also appear to rely on many Western-produced components. According to data provided by the Center for Army, Conversion, and Disarmament Studies (CACDS), the Azart contains six components of foreign origin, including the Spartan-6 chip, which encrypts communications and is produced by the U.S. company Xilinx in Taiwan. As a dual-use item, the Spartan-6 is commercially available and can be purchased via AliExpress. Similarly, Russia's reconnaissance, command, and communications complex Strelets-M relies on seven components of foreign origin, including a chip produced by the U.S.-based Microchip Technology.

The dependence of Russia's military-industrial complex on foreign-manufactured microchips can be explained by at least two factors.

First, chips and chip microprocessors produced domestically by a small number of companies tend to be of inferior quality and sophistication to Western designs. Since the imposition of Western sanctions, Russian companies have been unable to officially purchase technologies from the United States and its allies participating in the sanctions regime, including the Taiwan Semiconductor Manufacturing Company (TSMC), on which Russian chip producers heavily relied (Whelan 2022). Replacing these components with Chinese options in some cases requires a complete redesign of electronic equipment and the restructuring of cooperation chains, which may take years to complete (Kuz'min 2022). Moreover, Chinese chips often lag behind the leading Western microchip designs. While certain chips (such as the Spartan-6, the TSOP66, and the LQFP64) found in the Russian-made Azart and 9M544 precision missile can be purchased via AliExpress, dependence on such commercially available elements can make Russian weapons systems less reliable and prone to failure (DefenseExpress 2022). For example, U.S. Deputy Secretary of the Treasury Wally Adeyemo has suggested that "nearly 40 percent of the less advanced microchips Russia is receiving from China are defective" (U.S. Department of the Treasury 2023).

Second, the Russian semiconductor industry cannot meet the high demand for these elements. According to late 2022 data, the country requires up to 30,000 plates of basic-level microchips per month, but only 8,000 such plates can be made domestically (Petrova and Galieva

2022). In January 2023, the government announced the launch of a new technology park in the country's Ulianovsk region as part of an effort to accelerate its semiconductor production (Titov 2023). Yet given the export controls, it is difficult to gauge what the park's production rate and the quality of its products will be.

Conclusions

Russia faces a number of tremendous challenges when it comes to semiconductor production and supply. The war in Ukraine has highlighted considerable weaknesses in the country's semiconductor supply chains, which are not fully independent, and thus not sovereign. The fact that international sanctions have particularly targeted the chips sector is no coincidence: if civilian industries have been hit, the military-industrial complex is fighting to ensure continued access to high-quality microchips for its weapons system. In this domain, sanctions-evasion techniques—such as the setting-up of illegal supply chains—play a role, though this is difficult to assess with precision. On the Ukrainian battlefield, the capabilities of the Russian armed forces will likely be jeopardized in the longer run. This particular issue might be relevant to gauging the actual strength of the Russia–China relationship, as Moscow has been expecting substantial technological supplies and support from Beijing, a desire seemingly in tension with China's relative caution regarding U.S. secondary sanctions.

About the Author

Dr. *Julien Nocetti* is an associate fellow at the French Institute for International Relations (IFRI), a researcher at GEODE Centre (Geopolitics of the datasphere, University Paris 8), and heads the Cyber Risk Governance chair at Rennes School of Business.

Bibliography

- Bezrukov, A. 2017. "Mirovoe pole boia" [A Worldwide Battlefield]. *Izvestia*, November 9, 2017. https://iz.ru/667647/andrei-bezrukov/mirovoe-pole-boia.
- Borisov, V. 2016. "Rossiiskaia elektronika v XXI veke: globalizatsiia i natsional'nye interesy" [Russian Electronics in the 21st Century: Globalization and National Interests]. Presentation at the 9th conference on the History of Technology and Museums, Moscow, December 6–8, 2016.
- Byrne, J. 2022. "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine" (London: Royal United Services Institute, August 8, 2022). https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine.
- Byrne, J., et al. 2022. "The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV" (London: Royal United Services Institute, December 2022). https://rusi.org/explore-our-research/publications/special-resources/orlan-complex-tracking-supply-chains-russias-most-successful-uav.
- Kuz'min, I. 2022. "Chipy pod sanktsiiami. Sposobna li Rossiia obespechit' sebia mikroelektronnoi." *Sekret Firmy, April 12, 2022.* https://secretmag.ru/technologies/chipy-pod-sankciyami-sposobna-li-rossiya-obespechit-sebya-mikroelektronikoi.htm.
- Conflict Armament Research. 2022. "Component Commonalities in Advanced Russian Weapon Systems." September. https://storymaps.arcgis.com/stories/239f756e2e6b49a5bec78f5c5248bf3d.
- Defense Express. 2022. "Na mikroskhemakh z AliExpress: 'analogovnietna' Sistema navedennia 'Tornado-S' z RF" [On Chips from AliExpress: 'Analog Network' Guidance System 'Tornado-S' from Russia]. August 03, 2022. https://defence-ua.com/weapon_and_tech/na_mikroshemah_z_ aliexpress_analogovnjetna_sistema_navedennja_tornado_s_z_rf_foto-8418.html.
- Dzhalilov, T., and N. Pivovarov. 2017. "Istoriia sovetskoi elektronnoi promyshlennosti (konets 1950-kh-1960-e gody)" [History of the Soviet Electronic Industry (Late 1950s-1960s)]. Presentation at the 4th International Conference on Information Technology in Russia and the Former Soviet Union (SORUCOM), Zelenograd, October 3, 2017.
- Global Trade Tracker Database. 2023.
- Government of the Russian Federation. 2020. "Strategy for the Development of the Russian Electronics Industry until 2030." January 17, 2020. http://government.ru/.
- Manners, D. 2022. "Russia's Backward Chip Industry." *Electronics Weekly*, April 19, 2022. https://www.electronicsweekly.com/blogs/mannerisms/dilemmas/russias-backward-chip-industry-2022-04/ .
- Petrova, V., and D. Galieva. 2022. "Chiponezavisimost' so skidkoi" [Chip Independence at a Discount]. *Kommersant*, November 15, 2022. https://www.kommersant.ru/doc/5667792.
- Putin, V. 2016. "Poslanie Prezidenta Federal'nomu Sobraniiu" [Presidential Address to the Federal Assembly]. Kremlin.ru, December 1, 2016. http://kremlin.ru/events/.

- "Russian Import Network Acquired Electronics through Companies that Supply Chinese Military and Western Manufacturers." *Kharon*, January 5, 2023. https://brief.kharon.com/updates/russian-import-network-acquired-electronics-through-companies-that-supply-chinese-military-and-western-manufacturers.
- Titov, S. 2023. "Chipichnyi put'" [Microchip Way]. *Kommersant*, January 9, 2023. https://www. kommersant.ru/doc/5759442.
- Tolkachev, S., and A. Teplyakov. 2018. "Import Substitution in Russia. The Need for a System-Strategic Approach." *Problems of Economic Transition* 60 (7): 545–577.
- U.S. Department of the Treasury. 2023. "Remarks by Deputy Secretary of the Treasury Wally Adeyemo on International Sanctions Against Russia." Press release, February 21, 2023. https://home.treasury.gov/news/ press-releases/jy1286.
- Volostnov, A. 2019. "Microelectronics Market Overview." Presentation at the SemiExpo 2019 Conference, Moscow, May 14, 2019. http://semiexpo.ru/.
- Whelan, J. 2022. "Computer Chip Industry Begins Halting Deliveries to Russia in Response to U.S. Sanctions." *Washington Post*, February 25, 2022. https://www.washingtonpost.com/technology/2022/02/25/ukraine-russia-chips-sanctions-tsmc/.

ANALYSIS

Can Russia's SORM Weather the Sanctions Storm?

Gavin Wilde (Carnegie Endowment for International Peace, Washington D.C.)

DOI: 10.3929/ethz-b-000621535

Abstract

Both Russia's digital communications sector and its electronic surveillance system, SORM, were heavily reliant upon Western-produced technologies prior to Moscow's war on Ukraine. Since then, Western sanctions and export controls have been putting necessary hardware and software increasingly out of Moscow's reach. Russia's repressive surveillance state thus faces uncertain prospects, as domestically or Chinese-produced tech may prove insufficient to fill the void.

Fifteen years before Edward Snowden leaked details about U.S. electronic surveillance capabilities, a young Russian journalist named Vika Yegorova came into possession of a document detailing Moscow's own efforts to monitor telephone—and, increasingly, digital—networks. Over the next two decades, the veil of secrecy surrounding Russia's "system of operational-investigative measures" (known by the acronym SORM) would lift, aided in large part by the work of investigative journalists Irina Borogan and Andrei Soldatov (Soldatov and Borogan 2015). Their findings, particularly against the backdrop of Moscow's renewed invasion of Ukraine in 2022 and subsequent technological and economic isolation from the West, raise questions regarding SORM's long-term viability.

Moscow's initial research and development (R&D) efforts for a widescale system of telephonic surveillance began in the mid-1980s, at what was then the Soviet Union's oldest security R&D facility, located in the Moscow suburb of Kuchino. At that time, the KGB's 12th Section oversaw the technical details of wiretapping and monitoring domestic telephone exchanges. Following the collapse of the Soviet Union, the KGB's main successor agency, the Federal Security Service (FSB), ultimately took the helm of the program, bringing it under its own similarly named 12th Center.

As analog, landline telecommunications systems were gradually replaced by digital, mobile ones in the mid-1990s, SORM capabilities evolved alongside them. For instance, by 1998, as email was becoming ubiquitous, Russian communications regulators proposed that all Internet service providers (ISPs) be required to install, at their own cost, SORM-enabling "black boxes": componentry allowing the FSB to snoop on their web traffic. Court orders would be required for eavesdropping on specific content, but the FSB would not be obligated to apprise third parties, including ISPs, about these orders (Soldatov 2013). The FSB would also serve as the sole licensing authority for the cryptography used by Russian providers, making most web traffic easily decipherable (authorities would later grapple with end-to-end encryption at the user level, which complicated monitoring efforts—see *BBC* 2018). By the turn of the century, these mandates had been enacted and all major Russian telecoms and ISPs were expected to adhere to them.

As Russia under President Vladimir Putin became more politically repressive, SORM requirements followed suit. The 2016 anti-terrorism legislation known as the "Yarovaya Laws" forced telecoms companies and ISPs in Russia to retain all content—voice, text, video, and images—for six months and metadata—to, from, timestamp, and location indicators—for up to three years, as well as to make this data available to the authorities upon request. The logistical costs of adherence to these regulations were to be borne solely by service providers. In 2020, the FSB started demanding unfettered, remote access to all user data without exception, as well as automatic decryption of their communications. In early 2021, the Interior Ministry's own law enforcement surveillance programs were consolidated and placed under the auspices of the FSB's 12th Center.

By summer 2022, the Digital Ministry had moved from merely imposing fines on non-SORM-compliant ISPs and telecoms to denying or stripping their operating licenses outright. Federal communications regulator Roskomnadzor began piggybacking on SORM infrastructure to block traffic from, and access to, thousands of Western websites and services. Moscow's long-running project to hive off its "sovereign internet" from any content inimical to Kremlin interests worked in concert with SORM to create a largely self-contained, more easily monitored, more pliant information ecosystem (Sherman 2021). In practice, the standard for digital communications in Russia—for which SORM is a centerpiece—is now "that which cannot be surveilled or censored will not be transmitted." For example, Moscow's shift from attempting to completely block the popular Telegram messaging app in 2018 to eventually adopting its widescale use by 2023 suggests some ability to decrypt traffic (Korsun 2022)—either with or without Telegram's assent (*The Moscow Times* 2017). Today, Moscow likely uses SORM for some vestigial surveillance reach into former Soviet republics (Privacy International 2013), as well as marketing SORM capabilities to friendly states in Latin America (Farah and Richardson 2022) and elsewhere.

Western tech appears to have played a key role in SORM's evolution. Maturing beyond mere telephonic interception to monitoring Internet traffic (called deep-packet inspection, or DPI) entailed massive data networking and storage requirements (called a storage area network, or SAN). American, Japanese, South Korean, and European firms are the major players in the global SAN market. Meanwhile, documents leaked to *TechCrunch* (Whittaker 2019) and *The New York Times* (Satariano, Mozur, and Krolik 2022) from 2019 to 2022 indicate that equipment from Finnish-based Nokia and U.S.-based multinationals Cisco and Procera were key to SORM operability. This is not necessarily unusual, as governments worldwide—including democracies with more transparent warrantry and judicial recourse—require digital networking products to facilitate interception programs for law enforcement agencies. However, the revelations gave the world a window onto Russia's degree of apparent dependency on foreign tech that contrasted starkly with Moscow's rhetoric about the need for "import substitution" and Russia's technological autarky.

Meanwhile, a domestic ecosystem of contractors and suppliers props up SORM. Through a series of mergers and acquisitions over the past decade, many of these entities were consolidated under the direct and indirect tutelage of a single figure: Uzbekistan-born Russian tycoon Alisher Usmanov. Among the 100 wealthiest people in the world, Usmanov reportedly maintained close links to both senior Kremlin and FSB officials and owned major stakes in the largest Russian telecoms company, Megafon. He was also a key partner for the Tsitadel conglomerate, which controls an estimated 60–80 percent of the companies that outfit SORM nationwide—among them MFI Soft, Norsi-Trans, and Special Technologies—and is staffed by former 12th Center officers (Kovalenko 2019). By all accounts, Tsitadel became the leading beneficiary of the "Yarovaya Laws."

Russia's renewed incursion into Ukraine in late February 2022 proved an inflection point. Within weeks, a host of Western tech firms voluntarily suspended operations in the Russian market or began a process of wholesale withdrawal. The exodus included Nokia, Cisco, and Procera, as well as other major players like Intel, Adobe, Hewlett-Packard, Microsoft, Dell, Eriksson, LG, Nvidia, Kyocera, Siemens, SAP, Oracle, Juniper Networks, and Samsung (Yale School of Management 2023). By some measures, tech companies comprised nearly one-fifth of this historic pullback. The drawdown scuttled the Digital Ministry's designs for a 5G rollout in Russia, leading many industry insiders to worry that withdrawal-related equipment shortages would cripple the country's mobile networks in the long term. For example, gear from Ericsson and Nokia—including everything from antennas to fiber-optic cabling—serviced nearly half of the total cellular base stations in Russia, a market which, in turn, comprised a mere 2–3 percent of their revenues.

Then came Western sanctions and export controls. A complex and coordinated wave of restrictions by the United States and 37 other countries aimed to choke off the supply of strategic technologies—including semiconductors and other microelectronics—to the Russian military. This included the United States' first application of its Foreign Direct Product Rule against an entire country (Froehlich 2022), with a view to substantially limiting Russia's access to foreign-assembled products that use U.S.-made software and hardware. While such restrictions have not (yet) broadly targeted the Russian telecommunications sector, there is ample reason to suspect that crucial componentry might be diverted by Moscow to service more immediate military needs. For example, Ukrainian officials have reported that chips from household appliances have been found in captured Russian tanks and downed drones. In a potentially related development, as the U.S. digital communications giant Cisco completed its exit from Russia in spring 2023, the company destroyed upwards of $23 million in unsold inventory and spare parts rather than see it inherited gratis by an increasingly repressive regime waging a brutal war on its neighbor.

The extension of SORM into occupied Ukrainian territory opened the door for the United States to designate the Tsitadel holding company and other suppliers in early 2022. Nor did Usmanov and his business empire escape the crosshairs. After freezing his personal assets soon after the onset of the war, in April the United States blocked any transaction with commercial entities "owned, directly or indirectly, 50 percent or more" by him, including Megafon. The European Union followed suit. Possibly in anticipation of the move, in early 2023 Usmanov announced his "retirement" from commercial activity (*Radio Svoboda* 2023) and began selling his stakes in major SORM-linked enterprises (*Vedomosti* 2022), while Moscow was reportedly angling behind the scenes for state-backed Rostelecom to acquire Megafon (*Interfax* 2023). Russian Digital Development Minister Maksut Shadaiev told *Interfax* in February that such a merger would expand territorial coverage by optimizing the distribution of scarce equipment, rather than having each provider service only their own network and subscriber base. He gave only a cursory nod to any potential antitrust concerns.

The lack of such consolidation has been a hindrance to SORM, even prior to—and irrespective of—sanctions and tech shortages. In the absence of a unified, state-run telecom, independent providers have long been able to drag their feet or satisfy only the bare minimum of SORM-related requirements, which assume a degree of technological interoperability and longevity that are often unrealistic in practice, per industry insiders.

Meanwhile, full compliance is costly. An investigation by Russia Business Consulting from 2016–2017 found that Roskomnadzor issued over 450 SORM-related administrative violations against over 200 providers and individuals during that period, detailing how the financial burdens of SORM implementation were prohibitive for all but the major players (*RBK* 2017). The FSB and the Digital Ministry in 2017 assessed SORM-related costs to industry to be upward of 4.5 trillion rubles (Zvezda 2017); the Russian Union of Industrialists and Entrepreneurs countered with their own estimate of over triple that sum (*Kommersant* 2018). In other words, both the politics and the economics surrounding SORM appear to have incentivized consolidation of the largest ISPs and telecoms (*Reuters* 2023a), as smaller outfits find the costs of SORM compliance and non-compliance alike prohibitive and lack the political sway of major competitors like Rostelecom, MTS, and Megafon (Soldatov 2019). If the latter indeed ends up under state ownership, it will signal once again Moscow's refusal to distinguish between spurring its tech sector and merely subjugating it (Epifanova and Dietrich 2022).

Ironically, greater state control over the telecoms sector would likely make the SORM program more vulnerable than ever to punitive Western sanctions and technological isolation. The longer Russia's telecoms run on hardware and software solutions for which no updates or services are forthcoming, the greater the technological debt burdens SORM will assume by extension. As industry analyst Roger Entner told *The Moscow Times* in April 2022, "Russia will be frozen in 2022, while the rest of the world will move forward. It could turn into a failing technology museum" (*The Moscow Times* 2022). More recent signs point to this becoming a reality, as both the Digital Development Ministry and industry insiders acknowledged in spring 2023 that a broad-scale 5G rollout across Russia is unlikely until at least 2030 (*Kommersant* 2023b)—blaming a lack both of foreign-made componentry and of domestic production capacity that might compensate for this. Whether companies like Ericsson are willing to license Russian-produced versions of their equipment is an open question (*Kommersant* 2023a), while so-called "parallel imports" (deCourville 2022) via third countries are subject to bottlenecks and crackdowns (*EurasiaNet* 2023; Caglayan and Spicer 2023).

Telecoms and ISPs are not the only entities on which Russian authorities piggyback to enable their widespread surveillance dragnet. In 2017, the Central Bank established the Unified Biometric System (UBS) to warehouse the millions of voice- and facial-recognition samples of the Russian banking sector's clients. Within four years, connecting to UBS and populating it with data had become mandatory for the financial sector. Late last year, President Vladimir Putin decreed UBS the exclusive repository for biometric data under the law, which now includes everything from fingerprints to street-level CCTV footage. He also delegated the entirety of UBS oversight and operational control to the FSB, which almost certainly intends for UBS and SORM to be mutually complementary. Such interoperability—including sufficient data-warehousing to support it (*Kommersant* 2022b)—seems unlikely in the short term.

Whether they can become so remains unclear. Even if the Kremlin decided to take on the billions of dollars in costs to swap out obsolescing Western tech in Russia's digital communications and surveillance infrastructure, it is unlikely that domestically or Chinese-produced gear could entirely fill the gap. For example, the Russian state-run newspaper *Kommersant* (2022a) reports that foreign-made computing servers comprise half the current Russian market. However, according to a recent study by the Bank of Finland Institute for Emerging Economies, the value of overall global technology imports to Russia plummeted by 30 percent from December 2021 to December 2022—including those from China, which fell by 10 percent (Simola 2023).

Dependency on China would bring its own risks, as outlined in a recently leaked memo from Russia's digital development ministry to national security officials dated summer 2022 (*The Moscow Times* 2023). The document warned of dangers not only to the functioning of critical information infrastructure, but also to the viability of homegrown tech firms, and suggested curbs on imports of Huawei and other Chinese kit. It also put Russia on a timeline of up to 24 months to avoid total reliance on Beijing (potentially a nod to dwindling stocks of key componentry). However, more recent analysis of trading data indicates that while China has been a lifeline for some key technology exports to Russia since the war began (Simola and Röyskö 2023), it simply cannot backfill the totality of newly unavailable gear (Byrne et al. 2022).

In this regard, however sincerely Beijing might reassure Moscow about the depths of their friendship, Western sanctions appear to have hamstrung Chinese tech giants like Huawei and ZTE from charging to the rescue of the ailing Russian tech sector. For example, while Huawei (unlike Ericsson and Nokia) will continue to maintain and upgrade installed equipment in Russia, it has curtailed Russian operations and halted new orders. Moreover, both countries' firms largely depend on global semiconductor producers and assemblers like Taiwan-based TSMC, U.S.-based Intel, and South Korea-based Samsung, which are thus far complying with Western-backed restrictions. This will limit the extent to which they can backfill Russia's mounting advanced technology deficits.

Ultimately, the FSB-led surveillance state envisioned by the Kremlin prior to the Ukraine war—and by the KGB in its Cold War heyday—is now beset by a potentially crippling web of dependencies. Much about the program remains shrouded in secrecy. However, available insights suggest that SORM's fate is largely anchored to that of the Russian tech sector. As costs rise, componentry becomes scarcer, and Western governments zero in on enabling entities like Tsitadel, the coverage and capacity of the FSB's monitoring will likely suffer, too.

About the Author

Gavin Wilde is a Senior Fellow in the Technology and International Affairs program at the Carnegie Endowment for International Peace, where he explores cyber and information conflict. He previously served as Director for Russia, Baltic, and Caucasus Affairs at the U.S. National Security Council and as a senior analyst within the U.S. intelligence community. He is a distinguished graduate of the National War College, where his studies focused on information warfare.

Bibliography

- *BBC.* 2018. "Russia Seeks to Block Telegram Messaging App." April 6, 2018. https://www.bbc.co.uk/news/technology-43668537.
- Byrne, James, Gary Somerville, Joe Byrne, Jack Watling, Nick Reynolds, and Jane Baker. 2022. "Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine." RUSI, August 2022. https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_0.pdf.
- Caglayan, Ceyda, and Jonathan Spicer. 2023. "Turkey Halts Transit of Sanctioned Goods to Russia—Exporter, Diplomat." *Reuters*, March 20, 2023. https://www.reuters.com/world/middle-east/turkey-halts-transit-sanctioned-goods-russia-exporter-diplomat-2023-03-20/.
- deCourville, Nick. 2022. "Russia Legalizes Shady 'Gray Market' for Tech Products in Effort to Skirt Sanctions." *The Mac Observer*, April 26, 2022. https://www.macobserver.com/news/russia-legalizes-shady-gray-market-for-tech-products-in-effort-to-skirt-sanctions/.
- Epifanova, Alena, and Philipp Dietrich. 2022. "Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World." *DGAP Analysis* 1 (February 2022). https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf.
- *EurasiaNet.* 2023. "Russia's Parallel Imports Hindered by Central Asia Bottleneck." April 10, 2023. https://eurasianet.org/russias-parallel-imports-hindered-by-central-asia-bottleneck.

- Farah, Douglas, and Marianne Richardson. 2022. "Dangerous Alliances: Russia's Strategic Inroads in Latin America." *INSS Strategic Perspectives* 41 (December 2022). https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/strategic-perspectives-41.pdf.
- Froehlich, Annie. 2022. "Foreign Direct Product Rule: Is Russia the Next Huawei?" Atlantic Council, February 3, 2022. https://www.atlanticcouncil.org/blogs/econographics/foreign-direct-product-rule-is-russia-the-next-huawei/.
- *Interfax.* 2023. "Rostelecom in Talks to Buy MegaFon—Paper." January 30, 2023.
- *Kommersant.* 2018. "Razgovor pod zapis'. Kak budet rabotat' zakon o khranenii abonentskikh dannykh." June 29, 2018, https://www.kommersant.ru/doc/3670738.
- *Kommersant.* 2022a. "Otechestvennye proizvoditeli obespechili Rossiiu serverami i sistemami khraneniia dannykh na 45-50%." December 28, 2022. https://www.kommersant.ru/doc/5756175.
- *Kommersant.* 2022b. "Tsodrazverstka." March 15, 2022. https://www.kommersant.ru/doc/5258236.
- *Kommersant.* 2023a. "Otsel' vvozit' my budem shveda." May 3, 2023. https://www.kommersant.ru/doc/5967047.
- *Kommersant.* 2023b. "V sviazi s vyshesviazannym." May 19, 2023. https://www.kommersant.ru/doc/5988542.
- Korsun, Konstantin. 2022. "FSB v kurse: pochemu riadovym ukraintsam i chinovnikam ne sleduiut pol'zovat'sia Telegram." Focus.ua, August 15, 2022. https://focus.ua/digital/525481-fsb-u-kursi-chomu-peresichnim-ukrajincyam-ta-mozhnovladcyam-ne-slid-koristuvatisya-telegram.
- Kovalenko, Anna. 2019. "Partner Usmanova monopoliziroval rynok proslushki dlia 'zakona Iarovoi.'" *The Bell*, August 7, 2019. https://thebell.io/partner-usmanova-monopoliziroval-rynok-proslushki-dlya-zakona-yarovoj.
- *The Moscow Times.* 2017. "FSB Goes After Telegram Encryption Keys, Founder Claims." September 27, 2017. https://www.themoscowtimes.com/2017/09/27/fsb-seeks-telegram-encryption-keys-founder-claims-a59085.
- *The Moscow Times. 2022.* "'Failing Technology Museum': Uncertainty for Russian Telecoms as Foreign Firms Flee." April 22, 2022. https://www.themoscowtimes.com/2022/04/22/failing-technology-museum-uncertain-future-for-russian-telecoms-as-foreign-firms-flee-a77464.
- *The Moscow Times.* 2023. "Sanctions-Hit Russia Wary of Over-Reliance on Chinese Tech – Bloomberg." April 19, 2023. https://www.themoscowtimes.com/2023/04/19/sanctions-hit-russia-weary-of-over-reliance-on-chinese-tech-bloomberg-a80875.
- Privacy International. 2013. "Lawful Interception: The Russian Approach." March 4, 2013. https://privacyinternational.org/blog/1296/lawful-interception-russian-approach.
- *Radio Svoboda*. 2023. "Usmanov soobshchil RSPP ob "otkhode ot aktivnoi deiatel'nosti." January 23, 2023. https://www.svoboda.org/a/smanov-soobschil-rspp-ob-othode-ot-aktivnoy-deyateljnosti-/32235558.html.
- *RBK.* 2017. "Vne proslushki: pochemu Roskomnadzor i FSB sudiatsia s operatorami sviazi." November 9, 2017. https://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53.
- *Reuters.* 2023. "Russia Approves Veon's Sale of Vimpelcom to Management—RBC, Citing Sources." February 1, 2023. https://www.reuters.com/markets/deals/russia-approves-veons-sale-vimpelcom-management-rbc-cites-sources-2023-02-01/.
- Satariano, Adam, Paul Mozur, and Aaron Krolik. 2022. "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.
- Sherman, Justin. 2021. "Reassessing RuNet: Russian Internet Isolation and Implications for Russian Cyber Behavior." Atlantic Council, July 12, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/.
- Simola, Heli. 2023. "The Shift in Russian Trade during a Year of War." *BOFIT Policy Brief* 9/2023. https://publications.bof.fi/handle/10024/52738.
- Simola, Heli, and Aino Röyskö. 2023. "Russia's Technology Imports from East Asia." *Asian Economic Papers* 22 (1): 1–10. https://direct.mit.edu/asep/article/22/1/1/114932/Russia-s-Technology-Imports-from-East-Asia.
- Soldatov, Andrei. 2013. "NSA Is No Match for the FSB." *The Moscow Times*, June 18, 2023. https://www.themoscowtimes.com/2013/06/18/nsa-is-no-match-for-the-fsb-a25059.
- Soldatov, Andrei. 2019. "Security First, Technology Second." DGAP Policy Brief, March 7, 2019. https://dgap.org/en/research/publications/security-first-technology-second.
- Soldatov, Andrei, and Irina Borogan. 2015. "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.
- Soldatov, Andrei, and Irina Borogan. 2022. "Russia's Surveillance State." CEPA, October 26, 2022. https://cepa.org/article/russias-surveillance-state/.

- *Vedomosti*. 2022. "Kholding USM prodaet IT-gruppu 'IKS kholding.'" March 2, 2022. https://www.vedomosti.ru/business/news/2022/03/02/911731-usm-prodaet-iks-holding.
- Whittaker, Zack. 2019. "Documents Reveal How Russia Taps Phone Companies for Surveillance." *TechCrunch,* September 18, 2019. https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/?guccounter=1.
- Wilde, Gavin, and Justin Sherman. 2022. "Putin's Internet Plan: Dependency with a Veneer of Sovereignty." Brookings, May 11, 2022. https://www.brookings.edu/articles/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/.
- Wilde, Gavin, and Justin Sherman. 2023. "No Water's Edge: Russia's Information War and Regime Security." Carnegie Endowment for International Peace, January 4, 2023. https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644.
- Yale School of Management. 2023. "Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain." June 23, 2023. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain.
- Zvezda, Sergei. 2017. "V Rossii vstupila v silu samaia zhestkaia chast' 'zakona Yarovoi'. Operatory potratiat rekordnye summy, a tseny vyrastut." *T-Journal*, June 30, 2018. https://tjournal.ru/tech/72992-v-rossii-vstupila-v-silu-samaya-zhestkaya-chast-zakona-yarovoy-operatory-potratyat-rekordnye-summy-a-ceny-vyrastut.

READING TIP

Introducing the Ukrainian Analytical Digest

We are pleased to announce the launch of the *Ukrainian Analytical Digest* (UAD), a bimonthly open access publication designed to present academic insights about and from Ukraine to a broad international audience. To this end, the UAD will provide expert analysis of current affairs focusing on background information and interpretation. Contributions to the UAD will undergo fast-track peer review by an editorial board of distinguished scholars and will comply with academic standards of quality and integrity.

Each issue will feature several analyses focusing on a broader topic. The first issue will address language usage and language policy. Further issues will look at the state of social science research on Ukraine, Ukraine's foreign and domestic policy, public opinion in Ukraine and the Russian occupation of Ukrainian territory.

The new journal will be distributed free of charge as a pdf-file by e-mail. You can subscribe here: https://css.ethz.ch/en/publications/uad/newsletter-service-uad.html. All UAD-issues will also be archived online at https://css.ethz.ch/en/publications/uad.html and http://www.laender-analysen.de/uad/. The latter website will offer indices by author and topic.

The UAD is jointly produced by the Research Centre for East European Studies at the University of Bremen (www.forschungsstelle.uni-bremen.de), the Center for Security Studies (CSS) at the ETH Zurich (www.css.ethz.ch) and the Center for Eastern European Studies (CEES) at the University of Zurich (www.cees.uzh.ch) in cooperation with the German Association for East European Studies (DGO) (https://dgo-online.org).

We are looking forward to engaging with authors and readers.

Eduard Klein, Jeronim Perovic and Heiko Pleines
(Initiators of the Ukrainian Analytical Digest)

ABOUT THE RUSSIAN ANALYTICAL DIGEST

The Russian Analytical Digest is a bi-weekly internet publication jointly produced by the Research Centre for East European Studies [Forschungsstelle Osteuropa] at the University of Bremen (www.forschungsstelle.uni-bremen.de), the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology Zurich (ETH Zurich), the Center for Eastern European Studies at the University of Zurich (http://www.cees.uzh.ch), the Institute for European, Russian and Eurasian Studies at The George Washington University (https://ieres.elliott.gwu.edu), and the German Association for East European Studies (DGO). The Digest draws on contributions to the German-language Russland-Analysen (www.laender-analysen.de/russland), and the CSS analytical network on Russia and Eurasia (www.css.ethz.ch/en/publications/rad.html). The Russian Analytical Digest covers political, economic, and social developments in Russia and its regions, and looks at Russia's role in international relations.

To subscribe or unsubscribe to the Russian Analytical Digest, please visit our web page at http://www.css.ethz.ch/en/publications/rad.html

Research Centre for East European Studies at the University of Bremen
Founded in 1982, the Research Centre for East European Studies (Forschungsstelle Osteuropa) at the University of Bremen is dedicated to the interdisciplinary analysis of socialist and post-socialist developments in the countries of Central and Eastern Europe. The major focus is on the role of dissent, opposition and civil society in their historic, political, sociological and cultural dimensions.
With a unique archive on dissident culture under socialism and with an extensive collection of publications on Central and Eastern Europe, the Research Centre regularly hosts visiting scholars from all over the world.
One of the core missions of the institute is the dissemination of academic knowledge to the interested public. This includes regular e-mail newsletters covering current developments in Central and Eastern Europe.

The Center for Security Studies (CSS) at ETH Zurich
The Center for Security Studies (CSS) at ETH Zurich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching, and consultancy. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.
The CSS combines research and policy consultancy and, as such, functions as a bridge between academia and practice. It trains highly qualified junior researchers and serves as a point of contact and information for the interested public.

The Institute for European, Russian and Eurasian Studies, The Elliott School of International Affairs, The George Washington University
The Institute for European, Russian and Eurasian Studies is home to a Master's program in European and Eurasian Studies, faculty members from political science, history, economics, sociology, anthropology, language and literature, and other fields, visiting scholars from around the world, research associates, graduate student fellows, and a rich assortment of brown bag lunches, seminars, public lectures, and conferences.

The Center for Eastern European Studies (CEES) at the University of Zurich
The Center for Eastern European Studies (CEES) at the University of Zurich is a center of excellence for Russian, Eastern European and Eurasian studies. It offers expertise in research, teaching and consultancy. The CEES is the University's hub for interdisciplinary and contemporary studies of a vast region, comprising the former socialist states of Eastern Europe and the countries of the post-Soviet space. As an independent academic institution, the CEES provides expertise for decision makers in politics and in the field of the economy. It serves as a link between academia and practitioners and as a point of contact and reference for the media and the wider public.

Any opinions expressed in the Russian Analytical Digest are exclusively those of the authors.
Reprint possible with permission by the editors.
Responsible editor for this issue: Fabian Burkhardt
Language editing: Ellen Powell
Layout: Cengiz Kibaroglu, Matthias Neumann, Michael Clemens
ISSN 1863-0421 © 2023 by Forschungsstelle Osteuropa an der Universität Bremen, Bremen and Center for Security Studies, Zürich
Research Centre for East European Studies at the University of Bremen • Country Analytical Digests • Klagenfurter Str. 8 • 28359 Bremen •Germany
Phone: +49 421-218-69600 • Telefax: +49 421-218-69607 • e-mail: laender-analysen@uni-bremen.de • Internet: www.css.ethz.ch/en/publications/rad.html