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

Nocetti, Julien

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Nocetti, J. (2023). Sanctions Calling: The Dire Prospects for Russia's Chips Industry. *Russian Analytical Digest*, 298, 2-5. https://doi.org/10.3929/ethz-b-000621535

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