PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Russia and Digital Surveillance in the Wake of COVID-19

PONARS Eurasia Policy Memo No. 650
May 2020

Paul Goode[1]
University of Bath

Russia's response to the current pandemic highlights its aspirations to become a world leader in facial recognition and artificial intelligence (AI). The adoption of self-isolation and digital pass regimes provides opportunities to showcase the country's growing network of "safe city" programs with video surveillance for crowd and traffic control, which in some cities includes facial and vehicle recognition capabilities. However, the practical effect has been to highlight its limitations while facilitating the rapid expansion of data collection on Russian citizens.

Building Population Databases

The Russian government views AI as a crucial area of development and international competition, particularly with China and the United States. President Vladimir Putin famously stated in 2017 that, "whoever gains a monopoly in [artificial intelligence] will rule the world." In recent years, Russia has promoted the growth of intelligent public administration and law enforcement systems, in particular through the expansion of "safe city" and "smart city" programs. AI development also represents a lucrative future source of patronage, which is increasingly valuable for preserving political control when the economy is stagnating. The market volume of AI and machine learning in Russia was estimated at $10.8 million in 2017 and predicted to skyrocket to $432 million by 2020. Perhaps indicative of the sector's patronage potential, Putin's daughter Katerina Tikhonova was appointed to lead a new AI institute at Moscow State University with starting investment totaling $59 million.

Despite its aspirations and possession of significant technological expertise, Russia lags behind the world leaders in AI development, lacking the vast troves of user data possessed by China and the market conditions found in the West. The rapid expansion of China's capabilities in AI owes much to the datasphere provided by WeChat (the dominant Chinese social media platform), government access to personal data traffic, and

[1] Paul Goode is Senior Lecturer in Russian Politics at the University of Bath.

a culture that is less sensitive to government surveillance.[2] Russia's approach to digital surveillance is characterized primarily by way of filtering internet activity—meaning that it is not yet able to replicate China's advantageous possession of population data despite its extensive system of domestic surveillance known as SORM ("System for Operative Investigative Activities").[3]

Russia's options for AI development are further limited by international sanctions and generally a lack of trust from private investors. Russia's business culture remains extremely protective of its advantages and companies are reluctant to advertise their successes in using AI for fear of competition. Advances in the private sector's development of AI are further slowed by the combination of insufficient computing power and low levels of automation. The state and state corporations have thus taken the lead in setting the agenda for AI development in Russia. These efforts began largely in 2015 with the creation of a consortium of more than 30 companies and academic organizations under the auspices of a branch of RosTec known as the United Equipment Building Corporation. The creation of a new Center for Artificial Intelligence to be hosted by the Moscow Institute of Physics and Technologies was announced in 2017 and started working in 2018 with a consortium of partners that includes state corporations like Sberbank, RosTelekom, Gazprom, the state railway company RZhD, and RosSeti. Other state corporations like Sberbank, RosAtom, and RosTelekom are working along with the Ministry of Construction, Housing, and Utilities and the Ministry of Digital Development, Communications, and the mass media in developing "smart cities" as part of the government's "digital economy" national project.

Russia's national AI strategy, adopted in October 2019, calls for an ambitious program for the development of AI through 2030, including the construction of a massive population database and the production of a proprietary hardware platform. The execution of the national AI strategy will be the responsibility of the Ministry of Economics, while state corporations like RosTec and Sberbank will play a leading role in implementation. RosTec includes NtechLab, which provides the facial recognition technology used by Moscow. Sberbank, led by former Minister of Economics German Gref, has developed into a major player in the domestic technology competition and is considered on par with Yandex in terms of expertise and personnel. It drafted Russia's national AI strategy together with the Ministry of Communications.

Digital Surveillance and COVID-19

In 2019, the Moscow mayor's office, together with Sberbank, initiated an "experimental legal regime" for developing AI with an emphasis on facial recognition, transport, and

[2] See: Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, Houghton Mifflin Harcourt, 2019.
[3] See: Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, PublicAffairs, 2015.

medicine, which took advantage of the more than 160,000 cameras that already watch the city's 12 million inhabitants. In January 2020, NtechLab's facial recognition system identified more than 200 Muscovites who broke mandated self-isolation regimes after foreign travel. After this seemingly successful trial run, Sberbank and RosTec were quick to use the pandemic as an opportunity to expand their reach.

Sberbank's Gref declared in February 2020 that his company was prepared to provide support to the Russian government for fighting COVID-19, including "providing instruments like AI and facial recognition for cases in which people's faces are covered by masks." Similarly, RosTec's Sergei Chemezov contacted all regional leaders directly, offering to help them to install similar facial recognition systems to fight COVID-19. According to NtechLab's Aleksandr Kabakov, large scale deployment in a short time would not be possible, but "monitoring of public zones (streets, parks, key transport objects) could be deployed in one or two months." Regional media reported dozens of instances of regions moving to link citizens' digital passes during quarantine to "safe city" surveillance networks (accessible by regional administrations as well as law enforcement) to identify cars and pedestrians violating quarantine. In the Krasnodar region alone, the regional authorities claimed to have identified 504,000 vehicles breaking quarantine in just the first day of the system's operation.

Despite this fast start, implementation of facial recognition and social tracking became strained under the growing crisis. In March, the Moscow city administration made a "social monitoring" app available for download that required users' photos and telephone numbers to activate. However, programmers on a Telegram channel dedicated to discussing information technology discovered that the app actually used an Estonian facial recognition service and sent users' photos to a German cloud storage company. City authorities denied that the app used foreign servers, though it soon disappeared from Google's app store and it was later announced that the app would only be made available to those recovering from infection at home. Moscow finally abandoned plans for widespread facial recognition and switched to a lower-tech method of distributing smartphones with a pre-installed "social monitoring" app to infected patients. The city authorities next introduced a digital pass system, but botched implementation led to massive, hour-long queues at metro stations. Widespread reliance on Telegram, which is banned in Russia, for vital pandemic information led Duma deputies to argue for lifting the blockade because it "hurts the government's prestige more than the app."

The surge in nationwide network traffic during the crisis has also put pressure on internet and telecommunications providers that are struggling to meet the storage requirements mandated by the so-called Yarovaya law requiring all internet providers, social media, and messaging services to store user data for three years and to grant authorities access to encrypted communications. As Russia's regions moved in April to meet Prime Minister Mikhail Mishustin's order that they implement phone-based geolocation digital pass systems, the Ministry of Digital Development proposed amending the law "On

Communications" to require the linking of biometric data to sim cards, which ought to facilitate facial recognition in crowds by integrating information from government and mobile provider databases. The burden on providers for tracking and storing user data will escalate yet again in July 2020 when all smartphones sold in Russia will be required to pre-install Russian-made, government-approved applications that include search, GPS, social networking, personal digital assistants, and public service and payment apps. Consequently, rather than significantly enhancing the availability of population data for linking facial recognition with other kinds of data, the surge in network usage during the pandemic has put pressure on the government to postpone the requirement to increase annually the storage of user traffic.

Finally, attempts to grapple with the pandemic have further exposed extreme regional variations, as regions with limited technological capacity for digital surveillance have adopted more coercive measures. In turn, these variations in capabilities and enforcement stimulate criticism of regional and local governments and feed opposition concerns. At one extreme, Nizhny Novgorod was one of the first regions to introduce a smartphone app that uses QR code scanning to manage residents' requests to go outside. However, "review bombing" of the region's tracking app led to its removal from the Google Play store. The regional government later claimed that it was deleted from the app store because it had been improperly categorized as "Finance" rather than "Medicine." Elsewhere, in Russia's northwest, Karelia's governor ordered the addresses of patients to be published online, including street and house numbers. At the other extreme, Murmansk opted for a low-tech solution: those patients confirmed to be infected were required to wear tracking bracelets for remote monitoring, similar to those used for house arrest.

AI for Export?

While the leaders in Russia's AI sector may have hoped to turn the pandemic into an opportunity, it is more likely that the pandemic will force a reckoning with its limitations. Russia's existing strengths stem from its widespread filtering of internet traffic throughout the former Soviet space and its ability to use social media to create narrative confusion and to spread disinformation. While these have proven to be efficient means for projecting power and disrupting politics in other countries, the present crisis reveals their shortcomings—not just domestically, but also relative to China's capacities in terms of availability of hardware as well as the vast amounts of training data necessary to support digital surveillance systems.

In the near term, it is likely that Russia will continue to lose ground to China in Eurasia, especially in exporting hardware for digital surveillance. In recent years, China has been particularly active in Central Asia and the Caucasus, extending soft loans for digital surveillance technologies produced by Chinese companies like Huawei and HikVision. To the extent that the pandemic has created an urgent demand for smart technologies like

facial recognition and heat-sensitive cameras, China is far better positioned to benefit. For example, Ukraine urgently sought to purchase more than $2 million worth of thermal-sensitive cameras from HikVision in order to help with controlling the virus, though the contract was quickly cancelled for improprieties.

In the longer term, Russia has the potential to leverage its existing SORM-based surveillance networks in Eurasia to create a datasphere that rivals China's. In theory, its existing capabilities also provide it with the means to slow China's advance in the region—for instance, by creating incentives for cooperation through the Eurasian Economic Union, by using information warfare to inflame nationalist sentiment in target countries, or by instrumentally mobilizing international norms and ethics to slow the adoption of competitors' digital surveillance technology. Such tactics could help Russia to "run out the clock" while levelling up to the competition. The operative question, then, is whether Russia has time to spare, as one of the most important lessons of the pandemic for the Kremlin is that the clock is already ticking.

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY