PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Chinese Artificial Intelligence Projects Expand in Eurasian Cities

PONARS Eurasia Policy Memo No. 540
September 2018

Erica Marat[1]
National Defense University

As a global leader in developing and using surveillance technologies, China is exporting its high-tech brand of authoritarianism to its neighbors in Eurasia. Chinese firms have been promoting their artificial intelligence (AI) and surveillance technologies and projects globally, and attracting customers in Armenia, Azerbaijan, Russia, Tajikistan, Ukraine, Uzbekistan, Kyrgyzstan, and Kazakhstan. All of the systems are part of the "smart city" and "safe city" concepts that have been gaining popularity around the world as a response to rapid urbanization. The approach relies on digital technologies to improve urban life, but the tools also offer a structure to potentially expand authoritarian control over people and public places.

Closed-circuit television cameras and facial recognition technologies are particularly sought products. Chinese tech companies have the strongest position in Eurasian markets in these types of capabilities thanks to their regional presence, long-term credit structures, and high tolerance for financial risk. China's expanding influence in the AI domain may potentially have a greater impact on the daily life of urban populations across Eurasia compared to its Belt & Road Initiative. While automated systems can improve rule of law by applying laws fairly, advanced technologies and deep troves of identifying data can pose a threat to citizens if oversight mechanisms are not properly in place. Furthermore, these systems may rival and even replace the Western-driven, values-based rule of law programs that proliferated in the 1990s and 2000s.

[1] Erica Marat is Associate Professor in the Department of Regional and Analytical Studies at the College of International Security Affairs, National Defense University. She is the author of *The Politics of Police Reform: Society against the State in Post-Soviet Countries,* Oxford University Press, 2018. The opinions, conclusions, and recommendations expressed or implied within this policy memo are those of the author and do not necessarily reflect the views of National Defense University, the Defense Department, or any other agency of the Federal Government.

Securitizing Public Spaces Through Artificial Intelligence

The Eurasian countries pursuing safe and smart city programs are following a course set by other developing countries as part of their effort to adopt and adapt neoliberal economic development policies. Across the continents, the technological bundles are marketed as a way to improve public safety and introduce e-governance, predominantly in urban areas. Similar Chinese technologies have already spread to Africa, Asia, Europe, and Latin America. The smart and safe city technology market will be worth $135 billion globally by 2021, and China is poised to become a global leader in AI technologies by 2030.

Huawei, one of three leading Chinese tech firms already working in the region, is in an international pack of contenders that are rapidly gaining on market leaders such as IBM and Cisco. As of 2018, Huawei has 60 smart city programs in 20 countries, though issues have been raised about the company's integrity. The firm has links to the Chinese government; the founder and president of Huawei, Ren Zhengfei, is a People's Liberation Army (PLA) veteran, and the company's linkages to the PLA's cyber warfare group were confirmed in a 2012 U.S. intelligence report. The U.S. government continues to consider Huawei (and ZTE) as security threats. The UK government's purchase of Huawei technologies was criticized by experts for potentially allowing Chinese companies to spy on British organizations and disrupt telecommunications. Just this past summer, Australia banned Huawei and ZTE from operating in its market. In Europe, municipalities that invite Chinese tech companies to bid on projects tend to combine foreign innovations with homegrown capabilities and oversight.

Ukraine is a good example of where new technologies have been hard at work. As part of its promoted smart city project, Huawei and HikVision installed 4,100 surveillance cameras in Kyiv to help law-enforcement agencies better monitor crowds. Cameras monitor activities in Kyiv's central Independence Square, along major city streets, and at river beaches and recreation areas in the metropolis. Over 60 of the cameras can read license plates and have facial recognition capabilities. The broader public does not appear to have input or oversight as to how and when the authorities access and use the data collected by these cameras.

The "Eurasian" Use of AI: Securing the Political Status Quo?

Like in Western countries, many post-Soviet governments seek to use cutting-edge technologies to enhance public safety and security. In the Eurasian context, the safe and smart city concept has become primarily associated with enforcing the rule of law by policing small-scale disorderly behavior. The sharp quest for modernity among Eurasian political elites to improve urban governance—despite not necessarily having appropriate financial resources, legislative support, or public oversight debates—has allowed Chinese firms to sweep in with ready-made technological solutions.

Over the past two decades, large urban areas across Eurasia underwent dramatic changes. Urban populations expanded due to migration, political life in urban centers intensified, and cities became centers of high economic wealth alongside deeply impoverished outlying neighborhoods. Cities are now showcases for national branding, spaces of intense identity contestation, and political transformations (sometimes violent). The quality of life slowly improved for most urban residents, but increased population density triggered a rise in crime, along with strains on transportation and infrastructure such as clean water networks.

Wealthier Eurasian states, specifically Russia and Kazakhstan, have been able to attract a somewhat larger pool of potential technology investors/providers to its major cities. However, for the most part, the former Soviet region is an open, competition-free zone for Chinese firms, which have been proactively ready to modernize public security infrastructure with new technology packages. Three China-based companies, Huawei, HikVision, and CASIC, lead in smart and safe city projects in the region. Huawei is particularly popular because consumers know the brand for its smartphones, which are cheaper than Apple or Samsung products.

In smaller countries with weaker economies, like Kyrgyzstan and Tajikistan, Huawei is basically the only available provider of AI profiling technologies. Unlike for Russia and Kazakhstan, expenses are an issue. Kyrgyzstan, for example, was only interested in purchasing from Huawei images of digitally identified offenders as opposed to handling lengthy videos of all recorded activities over time. In another example, Tajikistan will take two decades to pay off its $20.9 million loan to Huawei for installing security cameras in its largest cities (while relying on automated road-violation tickets for fund-raising). Both countries are essentially looking to use surveillance technologies to find, capture, and punish disorderly persons—and profit from crime through fees and penalties.

Whereas "smart" is only problematic in some contexts, "safe" inevitably reflects political divides. Calls to improve safety presume the existence of dangerous elements within a society, and with new employed technologies, public spaces become formally privatized or informally dominated by wealthier populations, while newly urbanized groups formerly dependent on farming, agriculture, and government subsidies find themselves marginalized in poor urban neighborhoods. How nefarious elements are identified often reflects the views of privileged groups within cityscapes who demand regulation of everyday behavior. Drawing from policing techniques based on international models, the authorities in Kazakhstan and Ukraine, for instance, appear to have selectively introduced "safe city" concepts to support the political goals of incumbent regimes.

Chinese technology companies' presence in Eurasia is expanding without broader public discussions of what exactly constitutes public safety and privacy, not to mention the geopolitical implications. Huawei often brokers deals directly with political officials

rather than with private sector firms. Major projects usually begin when the company invites top government officials to its headquarters to showcase its state-of-the-art facilities and its role in reducing crime in China. Also, to promote its products, Huawei carries out soft-power projects in the region. For example, upon securing a multi-year telecommunications project in Uzbekistan, it sponsored student exchanges, inviting ten Uzbek students to China to learn calligraphy. According to the firm, another four students were invited to participate in discussions on the Belt & Road Initiative.

In Kyrgyzstan, while privacy concerns are on the minds of officials promoting AI technologies, the potential risks associated with Chinese firms (and by proxy the Chinese government) accessing local data are largely ignored. There is a resigned sense that both Chinese companies and Beijing can and will inevitably gather intelligence if they so desire, but they believe that the benefits of collaboration with Huawei far outweigh the possible repercussions of Chinese access to Kyrgyz public activities. These measures seem poised to discriminate against certain elements in cityscapes such as internal migrants, ethnic minorities, and the urban poor.

Implications for the Rule of Law

Using smart technologies to solve public safety concerns offers a rival or even replacement option for the Western-driven rule of law programs that proliferated in the post-Soviet space in the 1990s and 2000s. Western donors presented a "rule of law" approach as the key to economic development and political democratization. With the exception of Georgia and Ukraine, Western rule of law programs shied away from expanding or modernizing the material base of law-enforcement agencies. Assistance was used to train and re-train police personnel. Now (Chinese) surveillance technologies offer the opportunity to enhance law enforcement by digital tools, rather than by promoting values-based approaches to policing and local governance. On one hand, this could signify a failure of the decades-long Western approach to law and order. On the other hand, digital monitoring may reduce corruption, such as among police officers on the street. After decades of engagement with Western governments and international organizations, countries like Ukraine, Armenia, Moldova, and Kyrgyzstan—all of which have held competitive elections and showcase diverse civil societies—still have law-enforcement agencies that operate based on Soviet-era practices of militarized control. A certain automation in rule of law in authoritarian states may be a successful move toward fair governance practices.

However, the lack of "rules of engagement" and, moreover, the "China factor" in the employed technologies should not be overlooked. To preempt the impact of inevitable digitalization of urban life across Eurasia and the spread of virtual authoritarianism, Western donors and governments should share their policies about data usage and their information and analyses of Chinese companies' surveillance and AI capabilities. Such information exchange could take place with mid-level Eurasian government officials

who are responsible for procurement and policy implementation. Western and international NGOs could also share best practices in establishing oversight mechanisms of government purchases and use of surveillance and AI technologies, especially those based on Chinese software and hardware.

Conclusion

In order to implement digital control mechanisms quickly as a cure-all for urban crime and disorderly behavior, and to potentially keep an eye on mass gatherings, AI surveillance technologies are being rapidly implemented by Eurasian governments. They are rushing into the digital future and Chinese tech firms are conveniently positioned to step in quickly with solutions and credit. Lost along the way is serious due diligence.

The spread of Chinese AI surveillance technologies in Eurasia show how the region has been following the path of Western countries of expanding digital crime controls, even if high-tech solutions are not geared for all social problems. Since Chinese firms are now leading this development in the region, they may expand surveillance opportunities for both the national political elites and, potentially, for the Chinese government. Eurasian countries looking to leapfrog into the digital future are adapting virtual authoritarianism, with a lack of oversight legislation, which risks suppressing political dissent and further marginalizing already disadvantaged groups.

Governments in the post-Soviet region (along with Western donor agencies) should focus far more on the "smart" components of urban development—both digital and non-digital—that can help transform public places into more usable, comfortable, safe, and inclusive living spaces. Indeed, technology can help with self-governance through e-governance mechanisms, but what is less needed are rapidly deployed technologies that focus on ambiguous, digital, command-and-control capabilities, of which copious amounts of private data may be sent to local and national officials and Chinese policymakers. In many localities in Central Asia, rule of law can be improved without advanced surveillance technologies. The first step would be for municipal authorities to manage resources fairly and with consistent documentation, to be available for citizen feedback, and to apply their attention and resources to immediately improving public infrastructure, transportation, and air and water quality—especially in the poorer areas from which crime often stems.

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY