FIIA
BRIEFING PAPER

OCTOBER 2020 /294

DIGITAL AUTHORITARIANISM IN CHINA AND RUSSIA

COMMON GOALS AND DIVERGING STANDPOINTS IN THE ERA OF GREAT-POWER RIVALRY

Elina Sinkkonen
Jussi Lassila

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

DIGITAL AUTHORITARIANISM IN CHINA AND RUSSIA

COMMON GOALS AND DIVERGING STANDPOINTS IN THE ERA OF GREAT-POWER RIVALRY

- China and Russia are jointly advancing their shared interests in the international arena and are building up cooperation in the tech sector.

- Despite far-reaching plans, the asymmetry of cooperation in favour of China is increasingly at odds with Russia's national goals in digital technology.

- Differences in resources and standpoints are also reflected in the implementation of digital surveillance. China's surveillance system is sophisticated and extensive whereas Russia's is largely inconsistent and emerging, as evidenced by the fact that there was virtually no control of the internet in Russia until 2012.

- While advanced surveillance in authoritarian countries is worrying, technology in strategic sectors is also a key field of increasingly disconcerting great-power competition. As a result of strategic competition, the world is faced with the risk of technological decoupling, which would contribute to further fragmentation of the international community and deepening of existing rivalries.

ELINA SINKKONEN

Senior Research Fellow

Global Security Research Programme, FIIA

JUSSI LASSILA

Senior Research Fellow

The EU's Eastern Neighbourhood and Russia, FIIA

ISBN 978-951-769-661-6
ISSN 1795-8059
Language editing: Lynn Nikkanen
Cover photo: Pixabay

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7000
Fax +358 (0)9 432 7799

www.fiia.fi

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decision-making as well as scientific and public debate both nationally and internationally.
All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.

DIGITAL AUTHORITARIANISM IN CHINA AND RUSSIA

COMMON GOALS AND DIVERGING STANDPOINTS IN THE ERA OF GREAT-POWER RIVALRY

INTRODUCTION

China and Russia have become increasingly authoritarian in recent years, and the ways in which they can use technology to control their own citizens and to proliferate new surveillance methods to less developed authoritarian countries have caused concern. In July 2020, the law on mandatory preinstalled applications for smartphones, computers and smart TVs sold in Russia came into force. The new regulations were claimed to give Russian consumers domestic options, but critics are worried about information security and potential non-consensual information-gathering. China, for its part, passed a new regulation in December 2019 requiring all new smartphone buyers to scan their face before being able to use the phone. The regulation was framed as a part of larger efforts to ensure cyber safety by making it harder to access the internet incognito. These are only some of the recent examples of how authoritarian countries can use technology to monitor their citizens and boost domestic tech companies.

Global competition in technology is a tournament in which Chinese tech companies in particular take part. Great-power rivalry can be seen in US decisions to ban telecom companies Huawei and ZTE from its markets, and in pressuring European countries to restrict Huawei's market access as well. China has reacted to this by increasing its budget for the *Made in China 2025* programme and *China Standards 2035* initiative, and in trying to reduce reliance on US tech suppliers. China is also considering measures against Nokia and Ericsson, two European leaders in telecom networks, in case the European Union member states ban Huawei from taking part in building 5G networks in Europe. On October 20, 2020 Sweden announced that it will not allow Huawei or ZTE gear to be used by firms taking part in its 5G spectrum auction. The Chinese Foreign Ministry expressed its disapproval of Sweden's decision and urged Sweden to "correct its mistake ---to avoid negative impact on the Swedish businesses operating in China".[1] At the time of writing there is no information on any concrete countermeasures.

Meanwhile, the *Russian National Technology Initiative* from 2014 also builds on ideas of competing blocs, and more recent plans aim to elevate Russia's competence to that of a leading technological power. Echoes of great-power rivalry can also be heard in the context of internet regulations: Russia and China promote internet sovereignty and oppose the free flow of information. Many experts have speculated that the internet will be divided into two spheres, an authoritarian China-led one and a Western version.

This Briefing Paper overviews digital surveillance and tech investment strategies in China and Russia in the era of increasing great-power rivalry. Instead of inciting a threat narrative of an authoritarian alliance, discussion on technology cooperation between China and Russia should acknowledge differences between the countries and take into account other ancillary threats of which technological decoupling is a real and significant part.

DIGITAL SURVEILLANCE IN CHINA AND RUSSIA

Advances in technology point to more potent surveillance. Today's surveillance technologies range from cameras, drones and satellites to surveillance systems monitoring communications data. The essence of modern surveillance used for communications data is that programs are difficult to detect and easy to use remotely.

Authoritarian regimes that rely on digital surveillance and repression are identified as being among the most durable. During the last twenty years, the challenge of popular protests has become more consequential for numerous authoritarian regimes around the world. This has increased the need to monitor and suppress opposition via digital means to secure regime survival. Furthermore, the adoption of digital repression has not diminished the use of physical measures, as these new tools are used to identify and control opposition members more effectively.[2]

China is, perhaps, a prime example in many respects. The Chinese Communist Party has always taken social

[1] PRC Foreign Ministry, 'Regular Press Conference on October 21, 2020', https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825675.shtml.

[2] Kendall-Taylor, A., Frantz, E. and Wright, J. (2020), 'The digital dictators: how technology strengthens autocracy', *Foreign Affairs* 99(2): 103–115.

unrest issues seriously. Consequently, China has applied censorship of some sort ever since the internet became commercially available in the country in the mid-1990s. Internet surveillance is now one among many forms of surveillance and control in a society that is permeated by digitalization and, increasingly, artificial intelligence (AI). Digitalized visual surveillance is one such form. China has invested heavily in CCTV cameras with automated facial recognition programs. In Xinjiang, monitoring includes obligatory DNA sampling used for ethnic profiling.[3] Xi Jinping's regime has also built the capacity to forecast large-scale popular protests and has adapted its political indoctrination to the era of big data by using AI in surveillance and censorship.

In addition, China aims to resolve different societal and economic problems with an emerging "social credit system", driven by information technology. By collecting data from different sources, the social credit system can monitor, assess and change the behaviour of both citizens and companies. As state actors could not manage big data collection endeavours on their own, China's social credit system includes a wide variety of commercial actors. The system was supposed to be ready in 2020, but as there are data-sharing problems between different parts of the system and sanctioning mechanisms remain underdeveloped, the 2020 deadline will not be met. However, many parts of the system are already operational.

In post-Soviet Russia, the legal (or illegal) foundations of the state's surveillance practices were formed in the 1990s when the "System for Operative Investigative Activities" (*Sistema operativno-razysknikh meropriyatiy*, SORM) was introduced. SORM comprised the technical specifications for the lawful interception of telecommunications and telephone networks. It obliges all telecom operators to install hardware specified by the Federal Security Service (FSB), which enables comprehensive monitoring of communications. Although the original idea of using SORM was in line with Western practices in terms of legal control over the security services, its further use in the 21st century, also comprising the internet, has shown that the rule of law poses no impediment to the powers of the FSB and intelligence services in general. The aim is to keep all communications under mass surveillance using, for instance, so-called Deep Packet Inspection (DPI) technology, which seeks to map the content of conversations over the internet in great detail.

However, regardless of well-established foundations for the state's mass surveillance, SORM has faced financial and technological difficulties. In the absence of a single, state-controlled telecom operator, most independent operators have managed to "shirk" the requirements while appearing to be following them formally almost to the letter. As one specialist pointed out: "It's like a kind of Italian strike, where documents get passed back and forth for years but no one actually does anything."[4] A common technological challenge stems from the fact that networks built in the past are simply incompatible with the hardware that the authorities would like to use.

A partial indication of these difficulties is that there are no signs of the Kremlin's extensive capacity to control the information space, regardless of numerous shutdowns of allegedly harmful websites and acts of pressuring their authors. Indeed, the importance of the internet has grown at the expense of traditional state-controlled media (above all TV), regardless of ever-tightening internet legislation. Russian citizens are fully aware of protests, forest fires and ecological disasters around the country through the internet. In short, the state's increasing investments in developing mass surveillance have not resolved the fundamental problem of the free flow of information. In this regard, the Kremlin's main strength in controlling citizens is based on the deterrence provided by punishment and physical control over the offline space rather than on comprehensive digital surveillance.[5]

Although China has been viewed as an important partner by the Kremlin since the early 2000s, a major rapprochement has taken place within the (context of the) "authoritarian turn" in Russia since 2012. Underlying this turn is the longer-term drive to create a sovereign internet by 2024, for which China has been an important point of reference. However, as has been the case with SORM, administrative, resource-laden as well as societal challenges have been obvious here too. The main problem has been Russia's long-term integration into the global internet and the lack of functional and attractive national solutions compared to the widespread usage of Western technology and platforms (Apple and Google in particular).

[3] Qiang, X. (2019), 'The road to digital unfreedom: President Xi's surveillance state', *Journal of Democracy*, 30(1), 53–67.

[4] Operatory okazalis' nerazysknymi, *RBK* 9 November 2017, https://www.rbc.ru/newspaper/2017/11/09/5a03187e9a7947d88f988f53.

[5] Polyakova, A. and Meserole, C. (2019), 'Exporting digital authoritarianism: The Russian and Chinese models', *Democracy & Disorder*, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

China has invested heavily in CCTV cameras with automated facial recognition programs. *Source: Flickr/Steve Jurvetson (CC BY 2.0)*

Banning the internet and compensating for the lack of credible domestic carrots by applying sticks is not a viable solution. Whereas there are credible national equivalents for Western technology in China, and the use of the internet by citizens has always been under state control, there was virtually no control over the internet in Russia until 2012. When the wave of restrictive measures began that year, the proliferation of smartphones and the nationwide penetration of the internet forced the regime to adapt to ever-faster connections and the Western technology available to citizens. Measures to shut down allegedly harmful apps and the pressure against Western internet giants have proved largely ineffective. The most famous episode was an attempt to shut down the instant messaging service Telegram in 2018, which did not prevent the service from functioning, but ended up paralyzing millions of IP addresses, including governmental ones. In the summer of 2020, the blocking was officially stopped. Now the authorities are planning to prohibit the usage of the widely applied encryption technologies between user and site, as well as threatening to slow down Facebook and Twitter in Russia after refusals to hand over data on Russian users to the authorities.[6]

TECHNOLOGY IN CHINESE AND RUSSIAN INVESTMENT STRATEGIES

At the same time as China has conducted increasingly powerful surveillance, it has aimed to develop internationally competitive high-tech companies. China's industrial policy has emphasized support for innovation in strategically important sectors where certain companies receive preferential treatment and state subsidies. *The Wall Street Journal* reported in December 2019 that between 2008 and 2018 Huawei received 17 times more state assistance than Nokia, the

[6] Kukkola, J., Ristolainen, M. & Nikkarila J-P (eds.) (2017), *Game Changer: Structural transformation of cyberspace*, Finnish Defence Research Agency Publications 10, https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+10.pdf/5d341704-816e-47be-b36d-cb1a0ccae398/PVTUTKL+julkaisuja+10.pdf; Kukkola, J., Ristolainen, M. & Nikkarila J-P (eds.) (2019), *Game Player: Facing the structural transformation of cyberspace*, Finnish Defence Research Agency Publications 11, https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+julkaisuja+11+Game+Player.pdf/a4e38a00-e30e-cc48-f3af-d590655509ba/PVTUTKL+julkaisuja+11+Game+Player.pdf; 'Ministerstvo tsifrovogo razvitiya khochet zapretit' sovremennyye protokoly shifrovaniya v Runete', *Meduza*, 21 September 2020, https://meduza.io/feature/2020/09/21/ministerstvo-tsifrovogo-razvitiya-hochet-zapretit-sovremennye-protokoly-shifrovaniya-v-runete-togda-roskomnadzoru-budet-prosche-blokirovat-sayty; Rossiya gotovitsya nakazat' Facebook i Twitter zamedleniyem trafika, *The Bell*, 29 September 2020, https://thebell.io/rossiya-gotovitsya-nakazat-facebook-i-twitter-zamedleniem-trafika.

number two provider of telecom equipment.[7] "Innovation-driven development" has become a key priority in the Xi era, demonstrated, for example, in the *Made in China 2025* plan launched in 2015. The plan highlighted ten priority sectors including robotics, information technology, aircraft, aerospace technology and pharmaceuticals, in which China is aiming for global dominance by 2025 using a strategy combining import substitution and generous state financing.

Another important aspect of the innovation-driven development is the export of Chinese products and services, with the goal of not only gaining a market share but also trying to define technological standards through infrastructure investments. The *Belt and Road Initiative* (BRI) includes a project called the *Digital Silk Road*, which aims to propel China closer to the above-mentioned goals. Some even argue that Chinese measures of defining and exporting technological standards alter the global competitive landscape.[8] Through the BRI, for example, China promotes its satellite navigation system BeiDou, which reached global coverage in June 2020. However, Xi's industrial policy has not always been well received abroad, as can be seen in China's ongoing trade war with the United States, and the suspicions many Western actors harbour about allowing Huawei to construct parts of their 5G networks.

Russia relies on an explicitly more inward-looking and confrontational approach. The *Russian National Technology Initiative*, introduced in President Vladimir Putin's speech to the Federal Assembly in December 2014, draws on the idea of global competing blocs in trade, technology and politics. This document has since undergone numerous updates and roadmaps with which Russia intends to become "one of the three major technological states (along with the USA and China) by 2035". Due to a fundamental break with the West since 2014, the most natural partner has been China. However, this does not mean that Russia will in principle position itself as a partner of China, but rather that it will strive above all to be a leading player in the field of new technology from its own national starting points. The president's decree on the development of artificial intelligence in the Russian Federation, published in 2019, sees the future of artificial intelligence as a global struggle. The document points out that "the few leading players [not mentioned by name] in the global market for artificial intelligence are taking active steps to ensure their dominance in this market […] creating significant barriers for other market participants to achieve competitive positions". Relatedly, Russia's failure to do so is perceived to lead to economic and technological backwardness.[9]

SINO-RUSSIAN COOPERATION AND ITS LIMITS

China and Russia are jointly advancing their shared interests in the international arena and are building up cooperation in the tech sector. Although both countries are lagging behind the United States in most sectors of AI, China is catching up and aggressively recruiting new talent. Furthermore, there are certain sectors in which China and Russia are global technological leaders and can both benefit if cooperation deepens in the future. To give a few examples, a Chinese research team has made significant advances in developing entanglement-based quantum encryption in satellite communication, and Russia has advanced with regard to hypersonic weapons. Aircraft and aerospace technology are listed as key areas in the Chinese investment strategy, and there are some ongoing joint projects with Russia, such as building heavy-lift helicopters.

2020 and 2021 have been designated as years for Russian-Chinese science cooperation with the focus on communications, AI and the Internet of Things. While the nature of the cooperation has been largely symbolic, some tangible elements have started to accumulate over time. For example, the *Sino-Russian Joint Innovation Investment Fund* was established in July 2019, and various research and development projects have been launched. These include a project dedicated to sharing big data (*Sino-Russian Big Data Headquarters Base Project*) as well as projects using AI to facilitate cross-border commercial activities. In May 2019, the *Huawei Innovation Research Program* was launched in Russia, and Russian institutions have received 140 technological requests from the company in various areas of scientific cooperation. The involvement of Huawei can be considered by far the most significant demonstration of the technological cooperation

[7] Yap, C-W, 'State Support Helped Fuel Huawei's Global Rise'. *The Wall Street Journal*, 25 December 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[8] Zhao, S. (2020), 'China's Belt and Road Initiative as the Signature of President Xi Jinping Diplomacy: Easier Said than Done', *Journal of Contemporary China* 29 (123), 324.

[9] Natsional'naya technologicheskaya initsiativa, https://nti2035.ru/nti/; Ukaz Prezidenta RF ot 10 oktyabrya 2019 g. Nº 490 'O razvitii iskusstvennogo intellekta v Rossiyskoy Federatsii', http://www.garant.ru/products/ipo/prime/doc/72738946/.

declared between the countries in the fields of artificial intelligence, robotics and big data processing. The most significant dimension of Huawei's Russia collaboration is related to a potential implementation of the Russian Aurora operating system as a replacement for Android.[10]

The internet and its governance present another potential area for further cooperation. Internet regulation has been a subject of debate between private actors and states. In the 2012 Dubai World Conference on International Telecommunications, convened by the International Telecommunications Union (ITU), Western states lost out to authoritarian and developing states, which posited that regulation should be grounded in state-based politics at the UN specialized agency, ITU, instead of the more private Internet Corporation for Assigned Names and Numbers (ICANN), which allows participation by non-state actors.[11] China and Russia supported the ITU leadership. Both also support the sovereignty principle in internet governance, which they have promoted through the Shanghai Cooperation Organization and at the United Nations (UN). Their jointly drafted *International Code of Conduct for Information Security* was circulated at the UN General Assembly in 2015. China became the second largest contributor to the UN general budget for the 2019–2021 period, which increases its power in the UN sub-agencies dealing with internet regulation.

Overall, despite the cooperation, the asymmetry of the technological partnership in China's favour is causing increasing concern in Russia. Dependence on China in the high-tech sector does not serve Russia's efforts to develop its own digital technologies. There is already mounting concern in Russia that it will lose key talent to Chinese players. There is also a fear – common in Western countries – that China has the ability to steal foreign innovations and integrate them into its own production. In this context, there are plans to oblige Russian telecom operators to use domestic technology in the construction of the 5G network, which, however, is not currently available.[12]

CONCLUSIONS

In order to situate China-Russia cooperation in a broader context, it is helpful to remember two things. First, Sino-Russian cooperation is based on shared interests rather than ideology or shared values. It is difficult to find clear synergistic outcomes for Sino-Russian cooperation due to the asymmetry in the relationship in China's favour. China's de facto economic power underpinning its superpower status poses a key challenge to Russia's role in the potential technological decoupling between China and the West. Russia's own technology programs and knowledge base are aimed at developing credible national solutions, whereas China is export-oriented in striving to acquire know-how, conquer the market and set standards for Russia as well. In this respect, for Russia, China has begun to look more like a threat than an opportunity. At the same time, due to the widespread usage and popularity of Western technology in Russia, the country is more vulnerable to tensions between China and the US than it is dependent on its own national solutions. In a situation where Russia still lacks credible national solutions while technological decoupling is deepening between China and the US, the rift between Russia and the West will inevitably drive Russia to adopt Chinese technology.

Second, when it comes to problematic behaviour in the tech sector and surveillance, Russia and China are not alone. Non-state actors play a major role in this sector and authoritarian regimes are far from the only ones whose actions leave much to be desired from the viewpoint of citizens' privacy rights. Western countries sometimes sell surveillance equipment to authoritarian states and Western advertising companies help to build country brands for authoritarian countries. In most countries, new technologies are largely developed by private firms, making those with a dual-use potential in particular a grey zone in terms of regulation. The private surveillance industry sells surveillance technologies to governments, which use them against private citizens. The non-binding *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* added network communications surveillance systems and "intrusion software" to the list of dual-use technologies in 2013, but this has not significantly limited

[10] Bendett, S. and Kania, E. (2019), 'A new Sino-Russian high-tech partnership', *ASPI Report* 22/2019, pp. 1–21. See also https://career.huawei.ru/rri/en/.

[11] Nye, J. (2014), 'The regime complex for managing global cyber activities', Global Commission on Internet Governance, p. 7; Creutz, K, Iso-Markku, T., Raik, K. and Tiilikainen, T. (2019), 'The changing global order and implications for the EU', FIIA report 59, p. 54.

[12] Bendett, S. and Kania, E., 'The Resilience of Sino-Russian High-Tech Cooperation', *War on the Rocks*, 12 August 2020, https://warontherocks.com/2020/08/the-resilience-of-sino-russian-high-tech-cooperation/; 'Rossiyskiye operatory mogut lishit'sya vozmozhnosti stroit' seti 5G', *Vedomosti*, 20 September 2020, https://www.vedomosti.ru/technology/articles/2020/09/20/840535-rossiiskie-operatori.

sales of surveillance technologies for repressive purposes.[13] With new technologies acquired from Western markets, authoritarian states have committed human rights abuses against opposition members. Furthermore, the European Court of Human Rights has cases pending related to Western states' mass surveillance.

This is not to deny Chinese and Russian human rights abuses or other kinds of nefarious intrusions but to point out that projecting fears about new technologies solely onto authoritarian states creates a distorted picture of current realities. From the EU's perspective, technological decoupling and trade wars are also threatening. Public discourse on great-power competition and technological development should integrate all of these elements and avoid painting a black and white picture, which could serve to deepen existing grievances even further. /

[13] A/HRC/41/35 Surveillance and Human Rights. Report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736.