sciendo

Proceedings of the 6th International Conference on Economics and Social Sciences (2023), ISSN 2704-6524, pp. 681-689

The 6th International Conference on Economics and Social Sciences
Geopolitical Perspectives and Technological Challenges for Sustainable Growth in the 21st Century
June 15-16, 2023
Bucharest University of Economic Studies, Romania

Four Models of Digital Authoritarian Practices

Zoltán VÖRÖS[1], Khaled IMRAN[2*]

DOI: 10.24789788367405546-063

Abstract

To consolidate control within and beyond their borders, authoritarian regimes develop novel practices that allow them to apply digital communication technologies, surveillance techniques, Big Data analysis, and digital means of manufacturing public consent and spreading disinformation. When the practices are expanded and replicated beyond the regimes' borders, they are often labelled "exporting digital authoritarianism". In the last decade, China and Russia, with their palpable record of human rights violations, have been repeatedly accused of exporting digital authoritarianism, especially to other hybrid and authoritarian regimes. However, data-based surveillance practices and the export of surveillance software by Western democracies have often been off the radar. Based on secondary resources, this article proposes four models of digital authoritarian practices: Chinese, Russian, Western, and Imported. Despite some overlaps, these four models contain distinctive policies and practices. With its "Sharp Eyes" and "Golden Shield" initiatives that allow monitoring, recording, and analysing its citizens' real-time offline and online movements, the Chinese model is arguably the most institutionalised, digitally sovereign, and comprehensive. The Russian model, on the other hand, is dependent on tight information control, a strong and flexible legal regime, and low-cost, low-tech practices. In the West, government agencies and tech giants are using legal loopholes to carry out arbitrary data surveillance and extract huge amounts of personal data. Such practice is continuously undermining notions of human rights and legal and institutional capability and, in a way, albeit not to the degree of China and Russia, promoting authoritarianism. The last model, the Imported model, is followed by the smaller authoritarian and hybrid regimes, and naturally, their digital authoritarian practices are diverse. These regimes lack digital sovereignty and therefore depend on other states and companies for surveillance or disinformation campaigns.

Keywords: digital authoritarianism, surveillance, democratisation, China, Russia.

JEL Classification: F5, F52, F59.

[1] University of Pécs, Pécs, Hungary, voros.zoltan@pte.hu.
[2] University of Pécs, Pécs, Hungary, m1fm2w@tr.pte.hu.
* Corresponding author.

1. Introduction

In the 2000s, during the heydays of internet freedom, cyberspace was a libertarian dream come true, when state involvement was comparatively lower and individual liberty was higher than today. The freedom of cyberspace played a crucial role during numerous protests and social movements in the 2010s, from Occupy movements and the umbrella movement in Hong Kong to the so-called Arab Spring (Fuchs, 2014; Adorjan, Yau, 2015; Feldstein, 2021). However, one person's cyberactivist proved to be another person's cyberterrorist. States, irrespective of their nature, quickly acquired internet control and sophisticated digital tools to keep the public in check and maintain order (Pytlak, 2020). The state apparatus has to quickly cope with the fast-paced cyberspace, and in doing so, it sometimes undermines the basic notions of human rights, privacy, and dignity of individuals. Often, the legal provisions are not updated enough compared to the complexity of cyberspace. All these practices ultimately question the utility and primary objective of the state system: is the state for the people, or are the people merely subjects?

Therefore, this paper examines digital authoritarian practices and identifies the types of digital repressive mechanisms. Depending on the frequency of usage, this paper identifies four distinct models of digital authoritarian practice: Chinese, Russian, Western, and imported. It does not mean that a state belonging to one particular model exclusively follows the designated practices of the model. Rather, it means that the state predominantly follows the practices, along with the other practices followed by different models to a minor extent.

2. Digital Authoritarianism Goes Global

In the last few years, anglophone think tanks and media outlets have become increasingly concerned about the Chinese "export of authoritarianism' (Edel, Shullman 2023; The Washington Post, 2020; Polyakova, Meserole, 2019; Shahbaz, 2018). Such practice is sometimes labelled "tech-augmented" or "tech-enhanced" authoritarianism (Hoffman, 2022). Russia's export of surveillance software has also gained considerable attention (Polyakova, Meserole, 2019; Yayboke, Brannen, 2020). However, data-based surveillance practices and the export of surveillance software by Western democracies have often been off the radar. In addition, the states with limited technological capacity rely on these three sources, i.e., China, Russia, and Western states, and their implementation of digital repressive mechanisms is significantly different.

Digital technology advancements now provide governments with instruments to easily follow and monitor their people en masse, suppress opposition or protests, and manipulate public opinion. Such governments now have access to a larger range of repressive tactics thanks to technological advancements, which also lower the cost of repression (Dragu, Lupu, 2021). Naturally, these tactics should be the forte of authoritarian, repressive regimes, and in reality, they are. Researchers found that they are equally applied by liberal regimes, although the target is often not to suppress opposition but to protect people (Yayboke, Brannen, 2020). In this

article, it has been argued that digital authoritarianism is not practiced exclusively by authoritarian and illiberal democratic regimes, but also by liberal electoral democracies.

Moreover, since digital practices are ubiquitous, little work has been done to categorise them. Feldstein (2021) enlisted the practices and divided them into five broad categories: surveillance, online censorship, social manipulation and disinformation, internet shutdowns, and targeted persecution of online users. This paper adds another category to the above five: shaping international norms (Table 1). Digital authoritarian practices usually do not confine themselves within their own boundaries. Exporting digital authoritarianism is much easier than exporting authoritarianism. Powerful states are continuously trying to establish their dominant narrative of Internet governance in the international arena by supporting international conferences and establishing multilateral institutions. They also facilitate other authoritarian regimes by providing surveillance mechanisms and other repressive technologies. In a way, digital authoritarian practices tend not to confine themselves within territorial limitations; they are global.

3. Four Models of Digital Authoritarian Practices

3.1 The Chinese Model: Comprehensive, Overtly Institutionalised and Shaping International Digital Norms

In China, where the party state holds the ultimate regulatory authority, dissenting voices are muzzled and intimidated, and a pervasive state of surveillance has been established. Some scholars have identified China as the epitome of a "surveillance state" (Qiang, 2019; Chin, Lin, 2022). With the help of corporations heavily controlled by the Chinese Communist Party (CCP), Beijing is maintaining overarching state surveillance, censorship, and campaigns of misinformation (Wang, 2021).

Perhaps the nature of the Chinese model of digital authoritarianism is best understood in the province of Xinjiang, where targeted repression is preemptively carried out against , potential dissents using big-data analytics (Oztig, 2023). The Great Firewall of China, a network filtering tool used to screen Internet content, was built by the Chinese government in the 1980s, at the earliest days of the Internet (Chin, Lin, 2022). With the help of the Great Firewall, websites like Google, Facebook, YouTube, and Wikipedia are blocked, as are URLs, DNS, IP ranges, and VPNs (Qiang, 2019; Taylor, 2022). China blocked 700 websites and more than 9000 mobile applications in the first three weeks of 2019 (Polyakova, Meserole, 2019). The "Smart City" projects, with their extensive use of facial recognition, biometrics, and surveillance technology, monitor every move of a citizen in real-time (Hoffman, 2022). The Social Credit System is a national credit rating that measures the state-imposed "trustworthiness" of an individual or a business entity. Depending on their credit ratings, individuals and business entities are blacklisted and whitelisted, and their eligibility to receive certain services is determined (Cheung, Chen, 2021).

The Chinese model is perhaps the most comprehensive and institutionalised of all. In 2005, the Ministry of Public Security (MPS) and the Ministry of Industry and Information Technology (MIIT) launched the Skynet program to cover all the public spaces in China under the coverage of CCTV cameras (Polyakova, Meserole, 2019). The new Sherp Eye initiative, to ensure "no blind spot," is heading towards 100 % coverage of the Chinese public space (Thompson, 2021).

The CCP is already promoting its version of values and norms within its territory, primarily but not exclusively, with the help of the Social Credit System.

Table 1. Taxonomy of digital authoritarian practices

Surveillance	Online Censorship	Social Manipulation and Disinformation	Internet Shutdowns	Targeted Persecution of Online Users	Shaping International Norms*
Technologies, systems, or legal directives that enable control through identification, tracking, monitoring, or analysis of individual data or systems. Passive surveillance: Internet monitoring, mobile phone tapping, SIM registration, location monitoring, deep packet inspection, network interception, cable tapping, telecom surveillance. Targeted surveillance: intrusion operations which manipulate software, data, computer systems, or networks in order to gain unauthorised access to user information & devices (spyware/ malware). AI & big data surveillance: facial recognition, intelligent video, smart policing, smart cities/safe cities, social media monitoring. Surveillance laws: supports digital surveillance actions through the provision of intelligence & national security laws, data disclosure, data retention, and data localisation directives.	Laws, regulations, or actions undertaken by state authorities to restrict content & limit access to information. Content blocking and filtering Social media/ICT apps blocked. Takedown requests; content removal. Distributed Denial of Service (DDOS) attacks Infrastructure restrictions (Internet firewalls; closed ICT infrastructure – e.g., Great Firewall, Halal Net) Censorship laws & directives: religion/blasphemy, cybercrime, false news/fake news, political/hate speech, *lèse-majesté*, security/terrorism, copyright infringement, defamation/libel/sedition, indecency/anti-LGBT, financial targeting of groups	Strategies deployed by state or state-sponsored actors to shape narratives & beliefs and to mislead & manipulate users Disinformation Trolling, doxing, harassment Flooding Automated methods – bots, algorithms Vandalism and defacement	Intentional restrictions or disruptions of ICT networks or electronic communications rendering them effectively unusable for a specific period of time Total Internet shutdowns Partial shutdowns (restricted websites, blocked social media access) Throttling, blackouts, slowdowns	Online users persecuted by state authorities as a reprisal for posted political or social activity Online users charged, arrested, imprisoned, or in prolonged detention Online users physically attacked or killed	Support international conferences and organisations to facilitate their own version of Internet governance. Facilitate other authoritarian regimes by supplying surveillance and other technologies

Source: Feldstein, 2021, p. 26; *Added by the authors.

At the international level, China is promoting its own version of digital sovereignty by establishing the Shanghai Cooperation Organisation, providing training facilities to tech giants and the research community, and annually organising

the World Internet Conference. In this way, China is shaping the global norms of digital governance (McKune, Ahmed, 2018; Shahbaz, 2018). Moreover, China is one of the leading global suppliers of AI-powered surveillance technology and other repressive digital tools and software (Feldstein, 2021).

3.2 The Russian Model: Tight Information Control, Strong Legal Regime, Offensive, and Low-cost Alternative

Unlike the Chinese model, the Russian model is less strict and less comprehensive. This model uses surveillance mechanisms, but not to the degree of China; rather, Russia is more focused on censorship and information control. The Federal Security Service (FSB) analyses and conducts investigations when deemed necessary into all Internet traffic, telecommunications, and telephone networks throughout the country that is intercepted and stored via the SORM network (System for Operative Investigative Activities) (Akimenko, Giles, 2020). Moreover, Russia is developing the Runet, the Russian version of the Great Firewall, to block external internet traffic (Knake, 2020). Several government agencies are assigned to perform particular tasks. Department K under the Ministry of Interior is responsible for dealing with all sorts of general cybercrimes, and GosSOPKA is responsible for providing early warning and detecting cyberattacks (Akimenko, Giles, 2020).

The Russian model depends on a stronger and more flexible legal regime compared to the Chinese one. The latter is by no means without any legal provisions when digital repression is concerned, but it depends more on state agencies and arbitrary party directives than laws. The Russian regime enacted separate laws to ensure data localisation (On Personnel Data Law and amendments, 2015), VPN restriction (Information, Information Technology, and Protection of Information Law, 2017), criminalising reposting targeted content (Ant-Extremism Law, 2002), restriction on encryption (Amendments to Anti-Terrorism Law, 2016), and strategic censorship of contents threatening the regime (Internet Restriction Bill, 2012) (McKune, Ahmed, 2018).

Even though both countries possess pure cyber offensive capability, in practice, Russian activities are much more aggressive than China's. Russia regularly launches offensive disinformation campaigns and cyber-attacks on critical infrastructural systems and maintains strong cyber espionage capability (Brandt, Taussig, 2019; Akimenko, Giles, 2020).

Compared to China, Russia is still less digitally sovereign. Even a few years ago, Russia was dependent on China and western suppliers such as Cisco, Dell, and Microsoft (Kirilova, 2021). Gradually, Moscow is on the verge of gaining absolute digital sovereignty, and after the 2022 Ukraine invasion, it has gained momentum. Russian digital repressive tools are regularly imported by the former Soviet states, largely due to linguistic similarities, political ideology, and historical ties (Akimenko, Giles, 2020). However, Russian technology is a low-cost and easy-to-install alternative to most Chinese and Western systems. Therefore, African, Latin American, and Middle Eastern countries are the primary importers of these technologies (Codreanu, 2022).

3.3 The Western Model: State-industry Collaboration, Alienated from Accountability Mechanisms, and Shaping International Digital Norms

Digital authoritarian practices have always been considered the forte of authoritarian regimes like China and Russia, but evidence shows otherwise. Western liberal democracies are not lagging behind when surveillance and personal data monitoring are in question. Corporations such as Google, Amazon, and Facebook adopted a surveillance-based business model that monitors, collects, and sells our personal data, which is conceptualised as 'surveillance capitalism' by Shoshana Zuboff (2019). This model has come under severe fire from activist groups, journalists, and academics because it directly undermines a person's right to privacy, the right to equality and the non-discrimination, and right to free speech.

The ability of states and corporations to regulate, censor, and conduct cyberpolicing has considerably increased (Nye, 2011). These restrictions have included the virtual demarcation of virtual national borders, by separating national networks from the global Internet, which does not have any practical difference with China's Great Firewall (Deibert et. al., 2011).

Three dominant forces are still fighting over establishing their own version of internet governance: the Chinese model that advocates absolute government control, the US model that advocates an unrestricted free market and allows corporate dominance, and the EU model that advocates protecting individual privacy and personal data (Freedom House, 2021; Codreanu, 2022). Despite their own differences, the latter two models comprise of the Western model of Internet norms, that is detering Chinese attempt to shape international digital norms.

3.4 The Imported Model: Depends on Social Manipulation, Internet Shutdowns, Targeted Persecution, and Less Digitally Sovereign

Developing digital authoritarian mechanisms requires sophisticated technological know-how and huge funds. Therefore, most countries have to rely on the big powers to exercise authoritarian practices. Understandably, the countries that fall under this model are less digitally sovereign. This means they possess limited innovative capacity.

They import digital repressive tools from a variety of sources, and their practices are not uniform as well. Interestingly enough, not only the smaller authoritarian and illiberal regimes, but also electoral democracies buy and use these mechanisms.

These countries rely predominantly on the ‚older' practices of digital repressive mechanisms, which include social media manipulation, internet shutdowns, and targeted persecution. This does not mean that they refrain from surveillance and censorship in any way. Feldstein (2021) identifies five key components of social manipulation. They are disinformation, trolling and harassment, flooding (the use of bots and algorithms), and vandalism. Likewise, there are different varieties of Internet shutdowns and targeted persecution. For the time being, they are not adopting sophisticated surveillance techniques like AI-powered targeted surveillance, but that does not mean that they will not apply them in the future.

4. Why Model Digital Authoritarian Practices?

The decline of democracies after 2006, which Larry Diamond (2020) called „democratic regression," naturally gave way to autocratic regimes. Lührmann and Lindberg (2019) claim that this „third wave of autocratisation" is unique in two ways: first, democracies are gradually declining under legal disguise; and second, autocratisation is no longer a sudden event, unlike older transformations (like a military coup). Therefore, it is really difficult to precisely identify the transformation of a democracy into an autocracy. Contemporary research on autocratisation and the ubiquitous multiparty elections around the world suggests that the current wave of autocratisation is more covert and slow than previous waves. Lührmann and Lindberg further argue that "we lack the appropriate conceptual and empirical tools to diagnose and compare such elusive processes" (2019, 1095).

Unfortunately, in conventional literature, the typology of authoritarianism has not changed much from the military-monarchical-one party-multiparty quad. This typology might be applicable in the old Cold War settings, but today's political reality has changed a lot. Of course, there are some seminal works that reframe the typologies (Wahman, Teorell, Hadenius) and develop comprehensive data sets (Geddes, Wright, Frantz, 2014; Magaloni, Chu, Min 2013), but these data sets could not incorporate the changing and fluid nature of authoritarianism. These four models help to identify an authoritarian regime disguised as an electoral democracy.

Democracy, following the ideals of the Enlightenment, endorses human dignity and freedom as its key components. However, the question of individual freedom and human dignity is often overlooked by both the agent and the structure, due to the proliferation of digital space in our lives. In the name of public security, digital autocrats easily enter and control our private lives. This proliferation is so fast that even if the political elites attempt to curtail it, the legal provisions cannot keep pace with the ever-changing digital practices. Identifying the particular model of digital authoritarian practice might help policymakers intervene before it is too late.

5. Conclusion

Digital authoritarianism will only become more potent and more widely disseminated if left uncontrolled as new technologies continue to be developed. More and more people, businesses entities, and governmental institutions become dependent on digital tools and the Internet. Similar practices are becoming more prevalent in democracies, despite the fact that democracies are more transparent in their actions and citizens can hold leadership accountable for abuses, even though China and Russia are the main users of digital technologies for oppressive purposes and the main exporters of digital authoritarian tools. However, the bar for what constitutes misuse of digital tools will be dramatically lowered for digital authoritarians if liberal democracies continue to accept local or imported forms of digital authoritarianism. Democracies should work to monitor the conduct of digital authoritarians as well as their own online behaviour, even while promoting examples of democratic internet governance.

References

[1] Adorjan, M., Yau, H.C. (2015). Resinicization and Digital Citizenship in Hong Kong: Youth, Cyberspace, Claims-Making, *Qualitative Sociology Review*, 11(2), 160-178.

[2] Akimenko, V., Giles, K. (2020). Russia's Cyber and Information Warfare, *Asia Policy*, 15(2), 67-75.

[3] Brandt, J., Taussig, T. (2019). Europe's Authoritarian Challenge, *The Washington Quarterly*, 42(4), 133-153.

[4] Cheung, A.S.Y., Chen, Y. (2021). From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications, *Law And Social Inquiry*, 47(4), 1137-1171.

[5] Chin, J., Lin, L. (2022). *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*, New York, St. Martin's Press.

[6] Codreanu, C.M. (2022). Using And Exporting Digital Authoritarianism: Challenging Both Cyberspace and Democracies, *Europolity*, 16(1), 39-65.

[7] Deibert, R.J., Palfrey, J.G., Rohozinski, R., Zittrain, J. (Eds.). (2011). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Cambridge, MIT Press.

[8] Diamond, L. (2020). Democratic regression in comparative perspective: scope, methods, and causes, *Democratization*, 28(1), 22-42.

[9] Dragu, T., Lupu, Y. (2021). "Digital authoritarianism and the future of human rights". *International Organization*, 75(4), 991-1017.

[10] Edel, C., Shullman, D.O. (2023, April 19). How China Exports Authoritarianism: Beijing's Money and Technology Is Fueling Repression Worldwide, *Foreign Affairs*, accessed April 20, 2023, https://www.foreignaffairs.com/articles/china/2021-09-16/how-china-exports-authoritarianism.

[11] Feldstein, S. (2021). The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance, New York, Oxford University Press.

[12] Freedom House (2021). Freedom on the Net 2021: The Global Drive to Control Big Tech., *Freedom House*, accessed April 20, 2023, https://freedomhouse.org/report/freedom-net/2021/global-drivecontrol-big-tech.

[13] Fuchs, C. (2014). OccupyMedia!: The Occupy Movement and Social Media in Crisis Capitalism, Alresford, Zero Books.

[14] Geddes, B., Wright, J.A., Frantz, E. (2014). Autocratic Breakdown and Regime Transitions: A New Data Set, *Perspectives on Politics*, 12(2), 313-331.

[15] Hoffman, S.N. (2022). China's Tech-Enhanced Authoritarianism, *Journal of Democracy*, 33(2), 76-89.

[16] Kirilova, K. (2021). Russian Authorities Seek Total Control Over Internet, *Jamestown*, September 15. accessed April 20, 2023, https://jamestown.org/program/russian-authorities-seek-total-controlover-internet/.

[17] Knake, R.K. (2020). Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity, *Council on Foreign Relations*, September 2020, accessed April 22, 2023, https://cdn.cfr.org/sites/default/files/report_pdf/weaponizing-digitaltrade_csr_combined_final.pdf.

[18] Lührmann, A., Lindberg, S.I. (2019). A third wave of autocratization is here: what is new about it?, *Democratization*, 26(7), 1095-1113.

[19] McKune, S.L., Ahmed, S. (2018). Authoritarian Practices in the Digital Age. The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, *International Journal of Communication*, 12, 3835-3855.

[20] Magaloni, B., Chu, J., Min, E. (2013). *Autocracies of the World, 1950-2012 (Version 1.0)*. Dataset, Stanford University.

[21] Nye, J. S., Jr. (2011). *The Future of Power*, New York, Public Affairs.

[22] Oztig, L.I. (2023). Big data-mediated repression: a novel form of preemptive repression in China's Xinjiang region, *Contemporary Politics* (online), doi: 10.1080/13569775. 2023.2203568.

[23] Polyakova, A., Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Brookings*, August 2019, accessed April 20, 2023, https://www. brookings.edu/wpcontent/uploads/2019/08/FP_20190827_digital_authoritarianism_po lyakova_meserole.pdf.

[24] Pytlak, A. (2020). In search of human rights in multilateral cybersecurity dialogues. In Eneken Tikk and Mika Kerttunen (eds.). *Routledge Handbook of International Cybersecurity,* 65-78, London and New York, Routledge.

[25] Qiang, X. (2019). President XI's Surveillance State, *Journal of Democracy*, 30(1), 53-67.

[26] Shahbaz, A. (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. *Freedom House*, accessed April 21, 2023, https://freedomhouse.org/report/freedom-net/2018/rise-digitalauthoritarianism.

[27] Taylor, M. (2022). *China's Digital Authoritarianism: A Governance Perspective*, Chum, Palgrave Macmillan.

[28] The Washington Post (2020, August 5). China is exporting its digital authoritarianism, *The Washington Post*, https://www.washingtonpost.com/opinions/china-is-exporting-its-digital-authoritarianism/2020/08/05/f14df896-d047-11ea-8c55-61e7fa5e82ab_ story.html.

[29] Thompson, A. (2021, March 2). China's 'Sharp Eyes' Program Aims to Surveil 100 % of Public Space – Center for Security and Emerging Technology, *Center for Security and Emerging Technology*, https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/.

[30] Wahman, M., Teorell, J., Hadenius, A. (2013). Authoritarian regime types revisited: updated data in comparative perspective, *Contemporary Politics*, 19(1), 19-34.

[31] Wang, M. (2021, April 8). China's Techno-Authoritarianism Has Gone Global: Washington Needs to Offer an Alternative. *Foreign Affairs*, accessed April 19, 2023, https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritari anism-has-gone-global.

[32] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London, Profile Books.