Strong Yet Brittle:
The Risks of Digital Authoritarianism

Katherine Mansted, Non-Resident Fellow at the Alliance for Securing Democracy and Senior Adviser for Public Policy at The Australian National University's National Security College

May 28, 2020

Introduction

Authoritarian governments increasingly adopt technology-centric national strategies and methods of internal governance. They control their societies through digital censorship, propaganda, and surveillance, and use these same tools to manipulate foreign societies.[1] Their leaders prioritize the development of cutting-edge technologies in pursuit of government efficiency and military and economic advantage. Some analysts view this turn to "digital authoritarianism" as an approach designed to make authoritarians more durable at home and powerful abroad.[2] However, authoritarians adopt technology-centric strategies primarily due to their own insecurity. Digital authoritarianism is not so much a strategic choice, as it is a strategic necessity. In a globalized world, ideas and communications technologies are inherently threatening to authoritarian regimes, which must control both to ensure their survival. Authoritarians also increasingly depend on information technologies for economic growth and to build state capacity in areas where they have traditionally been at a comparative disadvantage to democracies. Ultimately, digital authoritarianism creates systemic risks for domestic governance and national security. In this sense, while digital authoritarianism has strengths, it will also become a regime's Achilles' Heel.

Why Authoritarians Become Digital Authoritarians

For all but the most closed, autarkic regimes, the corollary of being authoritarian in the information age is an ever-increasing need for information control and technology-centric approaches to domestic governance and interstate competition. This is for five key reasons.

Legitimacy

Authoritarian regimes must control information systems because otherwise, their citizens can share ideas, organize, and mobilize against them. Unlike democratic governments, which gain legitimacy from elections and constitutional checks and balances, authoritarian legitimacy hinges on (a) control, to suppress dissent or manufacture support, and (b) efficient outcomes, to stave off dissent or bolster support. The more of (b) the regime can achieve, the less (a) is needed (and vice versa). The internet and associated digital technologies are a direct threat to (a). For example, an influential 2017 essay by Chinese cyber strategists starkly observed that if the Chinese Communist Party (CCP) "cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term."[3] Paradoxically, the internet is also essential to achieving both (a) and (b). When the commercial Internet came to China in the mid-1990s, even as Party leaders understood its risks, they also recognized that it would provide more effective means for propaganda and surveillance (i.e. legitimacy via social control) and enhance intra-Party communications and economic opportunity (i.e. legitimacy via performance).[4] Authoritarian regimes, including China, Russia, Cambodia, Iran, and Vietnam, address this paradox by measures of control (censorship, market access restrictions, laws against certain speech, and temporary internet shutdowns) and propaganda. On social media platforms, authoritarian propaganda is often based on 'flooding' techniques that drown out dissent and make it harder for regime opponents to mobilize.[5]

Legibility

All bureaucracies—whether democratic or authoritarian—are attracted to technologies that make the societies they govern more legible and tractable.[6] In liberal democracies, structural checks and balances and a robust civil society counterbalance this impulse.[7] But authoritarian governments have few normative or structural brakes on when, and how, they use technology in service of the state. In societies that lack the feedback loops of representative democracy, independent media, and open public discourse, digitized social and economic interactions can simplify the business of governing; and create data-driven feedback loops to inform policy development and implementation.

Substitute for Civil Society

Advanced information technologies can be used to mitigate governance challenges caused by shallow civil society. Authoritarian regimes have traditionally been 'low trust' societies—a characteristic that imposes hidden transaction costs on economic interactions.[8] By design, they lack a robust, decentralized civil society—something economists and social scientists argue weakens state capacity.[9] Systems based on surveillance and enforcement, such as China's emerging social credit system, may help bridge authoritarians' trust deficit, obviating the need for more organic systems of social and institutional trust (which take time to develop and require a robust civil society).[10] Information technologies can also be used by citizens to expose corruption—a perennial concern for authoritarian governments. For example, the CCP takes a 'censorship lite' approach to social media posts that lets the regime keep tabs on local officials' performance.[11] Party leaders also tolerate certain kinds of online activism in order to boost government legitimacy and stability. For example, managed debate about local policies can give the appearance of public deliberation and support,[12] while allowing individuals to air grievances on social media can help the government to learn how to "satisfy, and ultimately mollify, the masses"—and, of course, to identify and punish dissidents, and prevent them from mobilizing.[13]

Technology as a Symbol of Progress

For some authoritarian regimes, the pursuit of high-tech modernism may be a motivating logic of its own. Chinese leader Xi Jinping has championed ambitious targets for China in frontier information technologies such as artificial intelligence (AI), quantum computing, and robotics. These are technologies that strategists and economists broadly agree will be key to military and economic power in the coming decades. Still, Xi's ambition for technological supremacy is also "an ideological end in itself," linked to the CCP's broader goal of demonstrating China's return to great power status.[14] Xi's targets can also be read as a continuation of the CCP's focus on "modernization," an objective to which authoritarian regimes—from Soviet Russia to Mao's China—have often coupled their legitimacy.

Competition with Liberal Democracies

Authoritarian governments—most notably Russia, China, and Iran—pursue technology-centric strategies in search of asymmetric advantages. Their strategists believe that information technology has been the key to decades of U.S. military, economic, and soft power dominance. There is truth in this belief. Until perhaps recently, U.S. signals intelligence enjoyed a self-acknowledged "home-field advantage," since much of the world's internet traffic passed through U.S. infrastructure.[15] At the same time, while the United States saw itself as leaving the internet to market forces, authoritarians viewed the U.S. "free and open" internet governance policy as inherently threatening. Without government intervention, the internet amplifies civil society voices (which are the wellspring of democracies' soft power advantage). It also enables protestors inside authoritarian regimes to mobilize (epitomized by the Arab Spring protests).[16]

The Vulnerabilities of Digital Authoritarians

While digital authoritarianism can enhance regime durability and national power, it also introduces deep-seated vulnerabilities, eight of which are considered below. Significantly, digital authoritarians may find themselves in a state of constant contest with other regime types, trapped in cycles of overreach and backlash, and prone to strategic miscalculations that pull them into interstate conflict. The current turn to digital authoritarianism therefore also has broader implications for international peace and stability.

Brittle Legitimacy

Reliance on information control makes authoritarians brittle. Small chinks in their information control armor could have existential consequences, particularly during political or economic crises (i.e. when the regime needs to rely on control for legitimacy because it is not delivering for citizens). The information and ideas most dangerous to authoritarians include:

- the identity of opposition groups and leaders and their levels of support; [17]
- technical means for subverting control of communications and surveillance technologies;[18]
- ideas about values that transcend state sovereignty, such as liberalism and human rights;[19]
- evidence that the central government is not delivering efficient outcomes;[20] and
- ideas that undermine the myths and narratives used to legitimize authoritarian rule or the power of the ruling elite.[21]

Constant Contest

Since technologies and ideas are dynamic, the battle for information control is a constant struggle. It can never be 'won.' Authoritarians are therefore in a perpetual state of information warfare, inside and outside their regime, and feel perpetually insecure. This dynamic may lead authoritarian governments to assess that it is worth engaging in information or cyberattacks to discredit liberal ideas at their foreign source or to shape or disable systems that jeopardize their information control—despite real risks of conflict escalation and global pushback.

Overreach and Backlash

The fundamental importance of information control to authoritarians increases the likelihood of overreach, leading to cycles of backlash and reprisal. Many perceive China's heavy-handed narrative warfare in Hong Kong and confrontational efforts to control narratives about coronavirus to be strategic missteps. For example, CCP efforts to stifle dissent by punishing online gaming company Blizzard and the National Basketball Association (NBA) arguably aided Hong Kong protester narratives;[22] while CCP obfuscation about coronavirus has prompted unprecedented diplomatic rebukes from world leaders.[23] Despite rising international awareness and condemnation of China's sharp power tactics,[24] China is accelerating, not muting, these behaviors.[25] One explanation for this is that the CCP calculates that the risks of international backlash (and occasional overreach by its officials) are acceptable, compared with the risk of letting domestic information control falter.

Impaired Feedback Mechanisms

Authoritarians embrace technology to increase the legibility of their societies. But legibility requires cooperation from society. It is facilitated by an open information ecosystem, robust civil society, mechanisms of transparency, and protections for political speech.[26] Conversely, information control and technology-enabled systems of surveillance and enforcement discourage accurate reporting and punish whistleblowing, while incentivizing officials to conceal failures and exaggerate successes.[27] In 2007, Le Keqiang (before he became China's premier) described China's national income figures as "man-made" and unreliable, and noted that more objectively verifiable proxies should be preferred to official statistics collected by provinces.[28] Without elections, authoritarians can also struggle to understand public sentiment, a problem highlighted by the Chinese government's mismanagement of massive ongoing protests in Hong Kong. Party leaders wrongly assessed that the protestors' grievances were primarily economic rather than political and that they did not enjoy broader public support.[29] As Zeynep Tufekci has observed, the costs of China's "authoritarian blindness" have been immense: a solvable issue (demands to withdraw a relatively unimportant extradition treaty) became "a bigger, durable crisis" with ongoing political consequences.[30]

China's delayed reaction to coronavirus is a stark example of the authoritarian legibility and feedback problem. Local officials and hospital administrators in Wuhan suppressed information about the outbreak and punished doctor whistleblowers—depriving other provinces and the central government (not to mention international authorities) of vital signals that would have allowed swifter action to control the pandemic.[31] Once authorities acknowledged the pandemic, China deployed the full weight of its digital surveillance capabilities. It was able to implement top-down lockdowns quickly; marshal its tech sector to build health apps; force citizens to download these apps; and access vast commercial holdings of personal data to cross-check compliance. However, it lacked critical bottom-up feedback systems that may have obviated the need for such draconian measures in the first place.[32] Indeed, controlling for income and population size, authoritarian regimes appear to be more lethal than democracies during epidemics, arguably because of their closed information ecosystems.[33]

Overreliance on Technological Systems which 'Fail Hard'

Many authoritarian governments are embracing AI-driven surveillance and control methods—from 'smart cities' to digital currencies, e-payment platforms and social apps. However, when AI systems fail, they tend to fail in unpredictable, often catastrophic ways. While citizens in democracies lament slow adoption of digital governance, authoritarians' speed comes with the risk that authorities roll out unsafe or vulnerable systems.[34] Imagine a critical failure of China's social credit system—whether by accident or sabotage—which affected the integrity of records. The implications for regime stability could be significant.

AI systems do not need to fail to produce problematic results. They draw insights and make predictions based on correlations in vast datasets but are not good at identifying causal mechanisms. This means that AI systems often produce outcomes which humans cannot reverse engineer or routinely evaluate. Like using asbestos to build a city, AI governance systems might produce good results in the short-term, but inconsistencies or oversights in their approaches could lead to cascading failures that humans struggle to identify, let alone rectify.[35]

Unintended Consequences from High-Tech Modernism

Fixation by central governments on achieving targets or deploying certain technologies creates incentives for local officials to deploy "technology placebos" that do little to address underlying economic and social concerns. For example, many so-called smart city projects in authoritarian societies have failed to meet development and economic goals. They are fraught with issues such as "unclear strategic goals" (e.g. they often optimize for surveillance, not development) and "inadequate implementation."[36] This problem may be particularly pronounced for less-developed authoritarian governments which have been persuaded, for strategic reasons, to buy Chinese-exported digital surveillance tools that are not customized to local circumstances. These cities may also become locked into unstable or insecure technical architectures[37] and economic dependence on China.[38]

Commitments to targets, and ideological fervor about technology, can also distort commercial decisions and raise unrealistic public expectations. Analysis of China's AI industry, for example, suggests that companies are eschewing investment in basic research and focusing on quick wins in applied research.[39] Additionally, China is already behind on meeting a number of its technology targets[40]—a lag that will likely be exacerbated by the global economic downturn following the coronavirus pandemic, and rising security fears in foreign markets about the security of Chinese technology and IP theft by its companies.

From a strategic perspective, there are risks that authoritarian governments' fixation on technology-centric strategies will lead them to overestimate what technology can in fact achieve. For example, Chinese military strategists have posited that AI could lift the 'fog' of war and eliminate uncertainty and confusion on the battlefield. This is an ahistorical and unlikely prediction that could inspire miscalculation.[41] Russian strategists theorize about how psychological operations might subdue adversaries without a shot being fired—an approach that may overestimate what cognitive warfare can achieve, at least without being combined with other elements of national power.[42]

Challenges to Social Cohesion

The medium- and long-term social consequences of digital authoritarianism are yet untested. Overreliance on surveillance and enforcement systems could attenuate relationships within a society, exacerbating authoritarians' underlying low trust problems. Since they tend to reduce citizens to data inputs, these systems may deny citizens' intrinsic desire for dignity and identity—with unexpected results.[43] Information control tactics—such as flooding—can repress opposition, but long-term may exacerbate public uncertainty and decrease business confidence and trust in official information, with implications for social cohesion and economic progress.[44]

Dysfunctional Innovation Ecosystems

Information control and state-led pushes for technology dominance risk hampering innovation. For example, to achieve Xi Jinping's 'Made in China 2025' goals, the CCP is supporting high-tech monopolies, restricting international collaboration, and yoking the state and market together.[45] However, monopolies are notoriously inefficient and cross-border collaboration is an important driver of innovation. Further, innovation works best under free market conditions and in open societies.[46] Some analysts argue that China's success in deploying AI applications is an exception to this rule. However, there is a risk that Chinese companies are prioritizing short-term breakthroughs (e.g. analyzing existing datasets to find new insights) at the expense of long-term investment in basic research.[47] While authoritarians may excel at developing and deploying AI applications, conceptual research is arguably the real engine of AI advancement—and something that will continue to thrive in open societies.

Summary and Further Research

All states face risks in the information age, but the extent to which regime type affects the relative likelihood of these risks materializing, and their magnitude, is understudied. For example, much has been written about liberal democracies' vulnerabilities to propaganda and foreign interference via social media.[48] But while information warfare against open societies is more *likely*, arguably it is a higher *magnitude* threat for authoritarians, where control of information is core to regime survival. Similarly, analysts often lament that democratic governments have been slow to digitize governance systems and craft forward-looking technology policy.[49] But while digital authoritarians might outcompete democracies in the roll-out of advanced technologies, this creates new vulnerabilities and risks. Inappropriate safeguards and accidents may result in cascading failures, while heavily digitized governance systems may be susceptible to foreign attack. Regime type may also affect the relative ability of authoritarians and democracies to mitigate their information age risks. For example, a democracy can build resilience to cyber and information threats through a variety of civil society and market-based interventions. Digital authoritarians must rely on a more limited set of top-down policy tools. Ultimately, a more systematic effort to map the comparative strengths and vulnerabilities of authoritarians and democracies in the information age could help both to better understand the other's threat perceptions and manage escalation risks. It might also highlight ways in which democracies can hold digital authoritarians' core interests at risk, in order to deter authoritarian interference in their own digital environments.

Endnotes

1. For an overview of the features of "digital authoritarianism," see Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and Chinese models," *Brookings,* August 2019.
2. See, for example, Andrew Kendall-Taylor, Erica Frantz & Joseph Wright, "The digital dictators: How technology strengthens autocracy," *Foreign Affairs,* March/April 2020.
3. Elsa Kania et al, "China's strategic thinking on building power in cyberspace," *New America,* September 25, 2017.
4. Geremie R. Barme and Sang Ye, "The Great Firewall of China," *Wired Magazine*, 1997. See also Rebecca MacKinnon, "Liberation technology: China's networked authoritarianism," *Journal of Democracy*, 22(2), April 2011.
5. See Margaret E. Roberts, *Censored: Distraction and diversion inside China's Great Firewall* (2018); Peter Pomerantsev, *Nothing is true and everything is possible: The surreal heart of the new Russia* (2015).
6. This analysis is informed by James C. Scott, *Seeing like a state: How certain schemes to improve the human condition have failed* (1998). For a helpful primer on the concept of legibility, see Venkatesh Rao, "A big little idea called legibility," *Ribbonfarm*, July 26, 2010.
7. Not always successfully. See discussions about "welfare surveillance" in democracies, for example in Jon Henley and Robert Booth, "Welfare surveillance system violates human rights, Dutch court rules," *The Guardian,* February 6, 2020.
8. Francis Fukuyama, *Trust: The social virtues and the creation of prosperity* (1995). See also Amy Webb, *The big nine: How the tech titans and their thinking machines could warp humanity* (2018).
9. Daron Acemoglu and James A. Robinson, *The narrow corridor: States, societies and the fate of liberty* (2019), 499-500.
10. "Is China's social credit system as Orwellian as it sounds?" *MIT Technology Review*, February 26, 2020.
11. Bei Qin, David Strömberg and Yanhui Wu, "Why does China allow freer social media? Protests versus surveillance and propaganda," *The Journal of Economic Perspectives*, 31(1), Winter 2017.
12. Rebecca MacKinnon, "Liberation technology: China's networked authoritarianism," *Journal of Democracy*, 22(2), April 2011.
13. Gary King, Jennifer Pan, and Margaret E. Roberts, "How censorship in China allows government criticism but silences collective expression," *American Political Science Review*, 107(2), May 2013, 14.
14. Julian Baird Gewirtz, "China's long march to technological supremacy," *Foreign Affairs,* August 27, 2019.
15. Glenn Greenwald, "NSA Prism program taps into user data of Apple, Google and others," *The Guardian*, June 8, 2013.
16. Valery Gerasimov, "The value of science in prediction," *Military-Industrial Courier,* February 27, 2013, trans. by Mark Galeotti in *In Moscow's Shadows*.
17. Henry Farrell and Bruce Schneier, "Common-knowledge attacks on democracy," Berkman Klein Center for Internet & Society, November 2018.
18. In 2015, Chinese hackers launched a massive distributed denial-of-service against the U.S.-headquartered website GitHub, which had hosted content that provided code to subvert the Great Firewall; an indication China is willing to use offensive cyber operations to suppress information that challenges its domestic control of information.
19. The notorious Document No.9, distributed to senior Party leaders in 2013, lists perils to CCP leadership including trends of "Western constitutional democracy" and "universal values" like human rights, media independence and civic participation: Chris Buckley, "China takes aim at western ideas," *The New York Times*, August 19, 2013. China is also taking a more "activist" role inside international bodies to "weaken" interna-

tional norms such as “human rights, transparency, and accountability”: Ted Piccone, “China’s long game on human rights at the United Nations,” *Brookings*, September 2018.

20. This may help explain China’s unprecedentedly confrontational approach to allegations it mishandled the coronavirus pandemic. See, for example, Laura Rosenberger, “China’s coronavirus information offensive,” *Foreign Affairs*, April 22, 2020.
21. Document No.9, referred to above, also listed “nihilist” criticisms of the CCP’s past as a peril to Party rule. Both Russia and China suppressed reporting of, and sought to discredit, the ‘Panama Papers’ leak, which revealed information about the offshore wealth of their ruling elite: “China steps up Panama Papers censorship after leaders’ relatives named,” *The Guardian,* 8 April, 2016; “Putin dismisses Panama Papers as an attempt to destabilise Russia,” *The Guardian,* 7 April, 2016.
22. “NBA faces backlash after ceding ground to China over pro-Hong Kong tweets,” *The Japan Times*, October 7, 2019.
23. For example, “Coronavirus: Macron questions China’s handling of outbreak,” *BBC News*, April 17, 2020; “Australia to use coronavirus suppression to push diplomatic weight,” *The Sydney Morning Herald,* April 20, 2020.
24. For more on the concept of sharp power see Christopher Walker, “What is ‘sharp power’?” *Journal of Democracy*, 29(3), July 2018.
25. See, for example, Laura Rosenberger, “China’s coronavirus information offensive,” *Foreign Affairs*, April 22, 2020; Ted Piccone, “China’s long game on human rights at the United Nations,” *Brookings*, September 2018.
26. Daron Acemoglu and James A. Robinson, *The narrow corridor: States, societies and the fate of liberty* (2019), 71.
27. Sarah Cook, “Beijing covered up COVID-19 once. It could happen again,” *The Diplomat,* April 13, 2020.
28. Peter Cai, “The data black hole threatening China’s economy,” *The Australian*, June 17, 2015.
29. Andrew J. Nathan, “How China sees the Hong Kong crisis,” *Foreign Affairs*, September 30, 2019.
30. Zeynep Tufecki, “How the coronavirus revealed authoritarianism’s fatal flaw,” *The Atlantic,* February 22, 2020.
31. Early research suggests that China could have prevented 95 percent of COVID-19 cases had quarantine measures been enacted three weeks earlier than they were (that is, when the late Dr. Li first raised an alarm about a new virus in December 2019): Shengji Lai et al, “Effect of non-pharmaceutical interventions for containing the COVID-19 outbreak in China,” medRxiv, March 13, 2020.
32. Yasheng Huang, “No, autocracies aren’t better for public health,” *Boston Review,* April 14, 2020.
33. “Diseases like COVID-19 are deadlier in non-democracies,” *The Economist,* February 18, 2020.
34. Paul Scharre, “Killer apps,” *Foreign Affairs*, April 16, 2019.
35. Jonathan Zittrain, “Intellectual debt: with great power comes great ignorance,” *Berkman Klein Center Medium,* July 25, 2019.
36. Jamil Anderlini, “How China’s smart-city tech focuses on its own citizens,” *Financial Times*, June 5, 2019.
37. Elsa Kania and Lindsey Sheppard, “Why Huwaei isn’t so scary,” *Foreign Policy,* October 12, 2019.
38. Bradley Jardine, “China’s surveillance state has eyes on Central Asia,” *Foreign Policy,* November 15, 2019.
39. Lorand Laskai and Helen Toner, “Can China grow its own AI tech base?” *New America,* November 4, 2019.
40. Craig Addison, “Why the Made in China 2025 road map to hi-tech supremacy will miss its deadline,” *South China Morning Post,* October 2, 2018.
41. See Elsa Kania, “Chinese military innovation in artificial intelligence,” Center for a New American Security, June 7, 2019, 29.
42. Peter Pomerantsev, “Inside the Kremlin’s hall of mirrors,” *The Guardian,* April 9, 2015.
43. Francis Fukuyama, *Identity* (2018).

44. As Adrian Chen and Peter Pomerantsev observe of Russia: “no one knows which parties or voices are genuine, and which are puppets of the regime, creating general paranoia and despair”: “The real paranoia-inducing purpose of Russian hacks,” *New Yorker*, July 27, 2016.

45. See “China’s integrated approach to indigenous innovation” in Elsa Kania, “Technological entanglement,” Australian Strategic Policy Institute, June 28, 2018.

46. Anne-Marie Slaughter, “America’s edge: Power in the networked century,” *Foreign Affairs*, January / February 2009.

47. Jonathan Zittrain, “Intellectual debt: with great power comes great ignorance,” *Berkman Klein Center Medium,* July 25, 2019. See also Lorand Laskai and Helen Toner, “Can China grow its own AI tech base?” *New America,* November 4, 2019.

48. See, for example, Joseph Nye, “Protecting democracy in an era of cyber information war,” Hoover Institution, November 13, 2018.

49. See, for example, Henry M. Paulson, “We’re letting China win the 5G race. It’s time to catch up,” *Washington Post,* December 16, 2019.