NBR

CONGRESSIONAL
BRIEFING SERIES

Confronting the Rise of Digital Authoritarianism

BY DOUG STRUB
THE NATIONAL BUREAU OF ASIAN RESEARCH

Digital authoritarianism has emerged as one of the major challenges facing the United States both domestically and globally. The United States' 2022 National Security Strategy highlighted this concern, noting the significant threat that digital authoritarianism poses to U.S. technology and innovation leadership. Evidencing the global nature of this challenge, Freedom House's annual "Freedom on the Net" report found that global internet freedom declined for the twelfth consecutive year in 2022 and that at least 40 countries blocked social, political, or religious content online—an all-time high in the history of the report.

Digital authoritarianism is generally defined as the use of digital and communications technology to engage in practices that prevent the free flow of information, repress political dissent, surveil citizens, infringe on personal privacy, subvert human rights and democratic principles, and facilitate malign influence campaigns domestically or globally. More broadly, it enables the spread of illiberal norms through virtual and physical digital environments. Many of these practices are not only being carried out by authoritarian actors within their borders but are also directly affecting liberal, open, and democratic societies—whether as a result of malicious digital activity from authoritarian states or through these societies' adoption of illiberal policies for their own perceived self-interest. It is imperative that Congress take a leading role in combating this trend.

Digital Authoritarianism in Practice

The People's Republic of China (PRC) has established itself as the vanguard of digital authoritarianism. Domestically, this is exemplified through its heavy use of digitally enabled censorship, state surveillance, and repression to aid the Chinese Communist Party in maintaining regime survival. Globally, the PRC also acts as the dominant force in spreading digital authoritarianism across borders. As demonstrated in the National Bureau of Asian Research's 2022 report "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order," the PRC is implementing a long-term, coordinated strategy to increase its control of and influence over the global digital domain.

A key component of this strategy is the export of restrictive digital norms, standards, policies, and legal frameworks through the Belt and Road Initiative (BRI) and accompanying Digital Silk Road (DSR). These initiatives seek to embed authoritarian values and practices at the core of developing countries' digital infrastructure and the digital ecosystems that operate on that infrastructure. Such efforts weaken the United States' power and influence abroad, undermine the economic and innovative capacities of liberal economies, and counter U.S. efforts to ensure open, reliable, and secure information and communications infrastructure globally.

Notably, digital authoritarianism is not carried out solely by authoritarian actors. Instead, it is implemented to varying degrees across a broad range of governance systems—including the United States, where high levels of freedom and openness can increase vulnerabilities to malign authoritarian activities. As evidenced through digital platforms such as TikTok, foreign governments can take advantage of open, globalized commercial domains to collect data, track U.S. citizens, and use algorithmic manipulation to influence information environments. These tactics also enable the spread of both misinformation and disinformation that can sow domestic distrust, spur division, and weaken democratic norms.

Enablers of Digital Authoritarianism

China's mass production of information and communications technology and surveillance equipment, fueled by government subsidization and unparalleled domestic demand, has facilitated the exportation of low-cost digital infrastructure around the world via the BRI and DSR. The result is increasingly advanced, affordable, and easily accessible technology that provides both authoritarian and nonauthoritarian governments the tools needed to leverage the digital domain as a means to increase control and influence. The export of these technologies advances restrictive norms and rules in recipient countries and often grants Chinese companies, and thereby the Chinese government, influence over data flows and storage. It also creates de facto technical standards on the ground, often establishing technological path dependencies and locking countries into future PRC-led digital development.

In addition to the rapid growth of connected individuals, the nature of these connections is also further enabling authoritarian tendencies in the digital domain. Smart cities, smart devices, and the Internet of Things have dramatically increased the types and quantity of data available, while also enabling the monitoring of users' everyday activities. This has been accompanied by the rise of new technologies such as artificial intelligence and facial recognition that have exponentially increased the ability of governments to analyze data to more effectively surveil and repress their citizens.

Options for Congress

As rapid technological advances and increasing global connectivity continue to introduce new challenges around privacy, surveillance, and digital influence, the most effective responses will require a whole-of-society approach, including legislative and regulatory action, private sector participation, and choices by individuals to oppose authoritarian practices and reject authoritarian technologies. But there are many steps Congress can take to make concrete progress toward stemming the impact of digital authoritarianism both in the United States and globally.

First, the United States could work to offer more competitive alternatives for digital infrastructure and digital development abroad to better compete with the BRI and DSR. The PRC's funding and construction of digital infrastructure abroad advances Beijing's illiberal digital vision by granting it greater influence over recipient countries' digital environments. The 2018 BUILD Act was a step toward countering this influence, and more recent efforts such as USAID's Enterprises for Development, Growth, and Empowerment (EDGE) Fund and the United States' participation in the Partnership for Global Infrastructure and Investment (PGII) seek new avenues to expand public-private partnerships to invest in development abroad. Congress can support such endeavors by ensuring that they are appropriately funded and prioritizing investment in digital infrastructure and the promotion of rules-based digital environments.

Second, Congress could enact a national data privacy protection law. Numerous competing visions of data governance have emerged around the world, including significantly divergent approaches even among likeminded countries. China, Japan, South Korea, and the European Union have all enacted comprehensive data protection regimes. The lack of a U.S. federal data protection law reduces the United States' ability to shape global norms and rules regarding data. The American Data Privacy and Protection Act, introduced in the 117th Congress, provides a foundation for the 118th Congress to make rapid progress on this issue.

A third step is to adopt a positive, proactive approach to digital rulemaking. Congress could utilize its role in shaping trade policy to ensure that the United States is pursuing a digital trade agenda that promotes an open, secure, and rules-based digital environment that accounts for human rights and democratic values while also facilitating trade and economic benefits for those who participate. The combination of the ongoing Indo-Pacific Economic Framework for Prosperity negotiations and the hosting of the 2023 Asia-Pacific Economic Cooperation (APEC) meetings provides a significant opportunity for the United States to make progress toward achieving meaningful digital trade rules in the region. The U.S.-Mexico-Canada Agreement and U.S.-Japan Digital Trade Agreement offer useful templates.

Congress could utilize its role in shaping trade policy to ensure that the United States is pursuing a digital trade agenda that promotes an open, secure, and rules-based digital environment that accounts for human rights and democratic values while also facilitating trade and economic benefits for those who participate.

Finally, the United States could increase and expand government programs and funding aimed at strengthening resilience against digital authoritarianism and its global spread. The rapid pace of technological advancement ensures that the tools and tactics of digital authoritarianism will be quickly and continuously evolving. To ensure that the United States is prepared to deal with new digital and technological challenges as they emerge, programs that expand U.S. understanding of these issues and enhance resilience against unforeseen digital and technological advancements are needed. Programs such as USAID's Digital Connectivity and Cybersecurity Partnership and the Advancing Digital Democracy initiative seek to strengthen digital norms and build cybersecurity capacity around the world. Numerous State Department programs work to combat global disinformation and provide crucial analysis on the root causes behind the spread of restrictive and authoritarian digital policies. Such programs are valuable tools in the contest over the digital domain, and Congress should both publicly voice support for them and ensure their continued funding. ~

Doug Strub is Director of the Center for Innovation, Trade, and Strategy at the National Bureau of Asian Research.

The views expressed are those of the authors.

Page 1: Pixabay. Page 2: Brendan Hoffman/Getty Images.