Stanford | Global Digital Policy Incubator
Cyber Policy Center

GLOBAL DIGITAL POLICY SNAPSHOT

COUNTERING THE RISE OF DIGITAL AUTHORITARIANISM: CHINA, AI AND HUMAN RIGHTS

NOVEMBER 2020

INSIDE THIS BRIEF:

- *Landscape: China's Domestic Abuses & Global Risks*
- *Human Rights Risks and Implications*
- *Recommendations for Policymakers & Democratic Governments*

INTRODUCTION

The global trend toward digital authoritarianism is one of the most significant emerging threats to human rights today. This trend entails the increasingly widespread use of digital technologies for repression at home, through surveillance, censorship and information manipulation; the export of technologies of repression abroad for these same purposes; and sophisticated international diplomatic efforts to undermine global commitment to human rights in digitized society. The most powerful and significant purveyor of digital authoritarianism is the People's Republic of China, perennially the world's worst abuser of internet freedom according to an annual assessment conducted by Freedom House.

Last month the Global Digital Policy Incubator concluded a four-part conference in partnership with the Human Rights Foundation, the Hoover Institution, and the Stanford Institute for Human-Centered Artificial Intelligence, titled "The Rise of Digital Authoritarianism: China, AI and Human Rights." The conference examined several aspects driving China's rise as an authoritarian digital power, and the full program included the following component themes:

- Part one: How AI is powering China's Domestic Surveillance State;
- Part two: The Ethics of Doing Business with China and Chinese Companies;
- Part three: China as an Emerging Global AI Superpower; and
- Part four: How Democracies Should Respond to China's Emergence as an AI Superpower.

Drawing on the insights from this conference and its speakers, this brief examines the threat of digital authoritarianism as modeled and exported by the PRC, and it provides an overview of the risks and implications for human rights. The brief concludes with recommended actions for democratic policymakers to counter digital authoritarianism globally. As former Secretary of State Condoleezza Rice noted in her introductory remarks for the conference, the challenge presented by China's ascending digital authoritarianism presents a significant threat to free peoples, and "democracies need to recognize we're in a race here, one that has huge implications for the future of humankind."

LANDSCAPE

In examining China's role in the rise of digital authoritarianism, it is useful to consider the government's behavior across two primary dimensions: (1) abuses and threats to Chinese citizens domestically; and (2) global risks posed by the PRC's export of digital authoritarianism to other countries, through both technology export and diplomacy at international fora to reshape global norms and standards in ways that enable authoritarian behavior in the digital realm.

China's Domestic Abuses

In examining China's practice of digital authoritarianism at home, there are three applications of digital technology that have been particularly integral to the Chinese Communist Party's abuses domestically.

The first is **censorship**. In China, the practice of online censorship is enabled in part by the Great Firewall, which (with the aid of technical mechanisms, such as deep packet inspection capabilities, DNS poisoning, VPN blockers, and IP address restrictions) blocks access to foreign media, websites and messaging applications and amounts to a highly complex censorship apparatus. Another feature of Chinese censorship includes content removal practices, wherein online criticism of the government is systematically removed from digital media. In addition, a particularly aggressive form of censorship is accomplished via offline arrests and consequences for internet activism and criticism, with support from legislation and regulations that tighten restrictions on online media. One example of this is China's national security law, which has been implemented in Hong Kong by imposing criminal liabilities against both users and social media companies for content deemed to reflect pro-democracy activism online.

A second, related application concerns government **control of the information space**. China's domestic information tactics include propaganda, but also the ability to control the tools, software, and infrastructure that comprise the digital media and communications ecosystem. Using these implements, the Chinese Communist Party can exert control by revoking access to information or revoking mobile and internet connectivity as punishment for activism. In addition, online manipulation floods the information space with paid commentary to drown out criticism.

A third element is **mass surveillance,** through which "China is creating a 360-degree view of its population," according to Xiao Qiang, a research scientist at UC Berkeley and Founder and Editor-in-Chief of China Digital Times. This surveillance system is multilayered. Maya Wang, senior China researcher at Human Rights Watch, noted, for example, that China has not only developed a national ID system, but on top of that has collected extensive categories of personal data, ranging from biometrics (including DNA, voice samples, and facial identifiers) to health records and even relatively mundane personal information, such as citizens' grocery store memberships. These elements combine to inform an elaborate Social Credit System, under which the government is able to leverage a coordinated administrative system to influence citizen behaviors through sanctions and public shame. As Xiao Qiang put it, the approach represents a new digital form of "totalitarianism that seeks to extend authority, through whatever means, over every aspect of [citizens] lives."

These cumulative surveillance efforts are supported by a combination of technologies, applications, and intensive human labor. Facial recognition technologies, for example, have enabled automated ethnic profiling, which both Wang and Paul Mozur, a technology correspondent for the The New York Times, noted has been used to monitor and subdue millions of Uighurs and members of other Muslim ethnic groups in Xinjiang. Surveillance is further powered by the Integrated Joint Operations Platform (IJOP), a labor-intensive "system of systems" used to surveil citizens. The government leverages the IJOP in part by using an app that collects and synthesizes data (including information ranging from gas usage to electricity usage and package delivery) about citizen behavior. Through this app, officials can receive reports of suspicious activities or circumstances, which may prompt official investigations. These forms of extreme surveillance extend across the country's different classes and cultures, with distinct initiatives, known as Skynet and Sharp Eyes, tailored to urban and rural environments respectively.

These three elements ––censorship, information control, and mass surveillance–– combine to enable the government to assert enormous power and influence over the lives of China's citizens, threatening human freedom, safety, and autonomy both online and offline, as described more thoroughly below. However, experts cautioned that while the government is exploiting technology in oppressive ways, it's important to recognize that these practices are not symptomatic of Chinese culture or societal values. As Xiao Qiang observed, the government's *China dream* is in fact the *Chinese people's nightmare*."

Global Risks

Beyond China's abuses at home, other important trends are contributing to the global environment of rising digital authoritarianism. Lindsay Gorman, the Emerging Technologies Fellow at the German Marshall Fund's Alliance for Securing Democracy, identified three such trends as particularly noteworthy. She framed the contest over technology as more than just about technology itself, but also a struggle between open and closed societies.

- The first trend is the growing confluence between economics and national power. This dynamic was echoed in a presentation by Mike Brown, Director of the U.S. Defense Innovation Unit, which highlighted the myriad ways in which that tech competitiveness now correlates directly with national power. This trend is particularly evident in the context of intellectual property theft––a prevalent issue throughout China's rise as a technology power––and also the massive state subsidies that the Chinese government has put into telecommunications firms like Huawei in order to achieve global competitiveness, which both Gorman and Brown highlighted. As Gorman put it, "What we're seeing now . . . is this idea that technological competitiveness is becoming a critical element of national power and . . . we're not really able to separate these two dimensions in the same way that we may have once been able to."

- The second trend, which is related to the first, is that national power is becoming less purely about military strength and increasingly correlated with soft power, including the ability to shape international environments through tech competitiveness and through power in the information arena. "Previously national security was more [directly] defined in terms of a nation's military strength," Gorman says, but the ability to shape global norms and governance and to exercise power in the information arena is now "emerging as a domain of competition between autocracies and democracies." While Mike Brown noted that the PRC is committed to neutralizing the United States' military advantages, this is now just one piece of a multi-pronged strategy to achieve global power. Evidence of this trend may be found by looking to China's Digital Silk Road strategy (a component of its Belt and Road Initiative, which Mike Brown noted can fairly be characterized as "an economic form of colonialism"), as well as the recent U.S. policy response to the PRC-based ownership of TikTok, which invoked national security authorities to justify a potential ban on the popular app in the United States.

- The third trend that Gorman identified is the use of data as an instrument of national power, both to assert control and also to amass resources that can fuel technologies of the future. By 2025 total global data "will be on the order of zettabytes [one sextillion bytes] . . . It's not about just adding more information and enabling a linear scale of applications," she noted. Once information reaches that scale, authoritarian governments have incentives "to extract as much data from citizens as possible, not only for purposes of oppression, but to power the next generation of emerging technologies." Eric Schmidt, former CEO and Executive Chairman of Google, contextualized this trend by noting that while China may enjoy certain data advantages––both in terms of the volume of aggregation, and its willingness to use data without concern for privacy standards––this does not necessarily equate to broader AI technological advancement, due to progress in the development of algorithms that require less training data to achieve the same learning. According to Schmidt, "the advantage for the moment may be with China in terms of its data aggregation, but that advantage ultimately may be less important than people think."

Taken together, these trends contribute to an environment in which the Chinese Communist Party is not only weaponizing data and emerging digital technologies to oppress its own citizens, but also is able to extend the reach of these risks beyond its borders.

China's export of surveillance technologies is a well-documented phenomenon of international concern. Conference participants indicated that surveillance technologies have been exported to countries including Ethiopia, Ecuador, South Africa, Bolivia, Egypt, Rwanda, and Saudi Arabia. China's facial recognition technology is in use, for example, on buses in Kazakhstan. Moreover, Chinese commercially-developed infrastructure and consumer technologies are in use in countless countries, including democracies in Europe and North America. China's distribution of technology and tools across borders not only enables illiberal governments to mimic the CCP model of digital authoritarianism at home, but also extends the potential reach of Chinese surveillance into other countries. During our conference, GDPi co-leader Larry Diamond moderated a thoughtful discussion of this issue with Chris Meserole (Brookings Institution), Anja Manuel (Rice, Hadley, Gates & Manuel LLC), and Christopher Balding (Fulbright University Vietnam), underscoring the complexity of the implications of, and potential responses to, the PRC's export practices.

China is also influencing the global landscape through its aggressive **use of international systems to reshape norms and principles**. A recent U.S. Senate report detailed the ways in which China has leveraged multilateral fora to institutionalize aspects of its agenda, erode human rights standards, and undermine a free and fair internet. These efforts reflect the ways in which the PRC's technological competitiveness can yield attendant soft power and economic influence internationally. Fora such as the UN Human Rights Council and the International Telecommunication Union risk being co-opted to institutionalize new authoritarian standards and practices with regard to digital rights.

In her remarks on the global landscape, Gorman described the future of the internet across three key layers: the infrastructure layer (such as 5G networks); the application layer (including technologies such as facial recognition, but also smart sensors, autonomous vehicles and other technologies that amass data); and finally, the governance layer (which includes the ways that China is using its technological competitiveness to shape international practices and principles in ways that align with its vision). The PRC is striving for dominance across all these layers not only at home but around the world. These features combine to ensure that China's digital authoritarianism poses significant risks on a global scale.

HUMAN RIGHTS RISKS & IMPLICATIONS

Among the primary human rights threatened by digital authoritarianism is **the right to privacy**. As both an instrument of oppression and an economic tool, widespread surveillance, coupled with the integration of various data (as illustrated by the social credit system) substantially diminishes the privacy of Chinese citizens as well as their humanity and autonomy, in part by substituting choice and decision-making with rote analytics. The risks to privacy are severe for all Chinese citizens but especially for Uighurs and other minority groups, who are subject to rigorous surveillance both within China and reportedly in expatriate communities abroad. And as noted above, these threats to privacy are compounded by the widespread export of Chinese surveillance technology to authoritarian regimes and fledgling democracies.

Digital authoritarianism also threatens **freedom of expression**. Widespread censorship of the internet, restrictions on access to information, and systematic removal of content ––as well as the regular arrest of those who speak out in even fairly mundane ways against the Chinese regime online––severely threaten the ability of citizens to freely express themselves online. These threats are exacerbated by significant manipulation of the digital information environment, featuring a flood of pro-government narratives that inhibit the ability of citizens to form opinions free from government influence. These risks have been further amplified by the COVID-19 crisis, during which the Chinese government has worked hard to control information about the pandemic.

The ubiquitous surveillance and strict restrictions on speech and information also pose threats to the **freedoms of assembly and movement**. Maya Wang noted, for example, that IJOP data collection mechanisms and facial recognition technologies are positioned at various geographic touchpoints, creating a virtual fencing effect that limits free movement among those communities. More generally, assembly that might potentially threaten the regime, or even challenge it on specific issues, becomes substantially riskier when citizens know the degree to which they are surveilled by the state. This is further amplified by reports that Uighurs and other minorities may be targeted even after they have left China. This means that limitations on freedom of movement are amplified by the knowledge that even once they have left the country, their surveillance by the state may continue.

Finally, China uses its digital infrastructure to threaten the **safety and security** of its citizens in a range of ways. Numerous human rights organizations have documented the repression and forced internment of Uighur minorities in Western China. The intersection of digital tools with this repression is profound, and includes tracking using social media; targeting the families of Uighurs who have left China; and use of virtual fences and IJOP applications to target Uighurs with extreme and invasive surveillance. Beyond the threats to these minorities, the CCP has used its digital surveillance apparatus against pro-democracy protestors in Hong Kong, targeting them for arrests and violence. China's repressive digital information laws have also resulted in the forced imprisonment of journalists and others who speak out against the regime.

RECOMMENDATIONS FOR POLICYMAKERS AND DEMOCRATIC GOVERNMENTS

1) Democratic governments should work collaboratively to reinvigorate the democratic alliance for the digital age. Democracies should act cooperatively to articulate a compelling alternative and a positive vision for a free and open digital future. This vision should include mechanisms for coordinating international responses to digital authoritarian threats. As Alex Stamos, director of the Stanford Internet Observatory, noted at our conference, the efficacy of policy responses such as export controls is substantially improved through international coordination. To enable this level of cooperation among democracies, former Google CEO Eric Schmidt encouraged government leaders to establish "an alliance on digital technology and values." In conversation with GDPi's executive director Eileen Donahoe at our conference, Schmidt emphasized, "This is an opportunity for diplomacy . . . [and] working in alignment will magnify our impact."

2) Democratic policymakers must implement a rights-respecting, values-based approach to technology development and governance domestically. Democratic governments should demonstrate the virtues of a values-based alternative to digital authoritarianism by adhering to such principles in their own policymaking. As Chris Meserole succinctly put it, "We have to get our house in order." To achieve this successfully, democratic governments should implement organizational safeguards to ensure that digital policy development in the domestic context is aligned with international principles of internet freedom. As part of this process, Lindsay Gorman suggested that "Democracies ... take a look in the mirror [and ask:] what elements of our own systems are potentially feeding repression?"

3) Democratic governments should clarify and elevate the risks of digital authoritarianism within the multilateral agenda. Democratic governments must meet China on the global multilateral stage, both to challenge closed concepts such as digital sovereignty, and to proactively use these international fora to advance the democratic model and principles of internet freedom. As the recent Senate Foreign Relations Committee report noted plainly, "From the United Nations (UN) to the World Trade Organization (WTO), China has used its political and economic muscle to shape the international standards surrounding the digital domain in favor of a more authoritarian view of the world." Democratic governments must counter these efforts in the multilateral sphere.

4) Democratic governments should prioritize investment in technological research and development. These investments will ensure the availability of future technological components that reflect democratic values, while simultaneously preserving democratic competitiveness and influence in the realm of technological governance and power. In her opening remarks to our conference, Condoleezza Rice stated, "We need to have a concerted effort on behalf of free peoples to ensure that the digital authoritarians don't win; they can't win the race for this technology, because whoever wins the race, is going to have a leg up on shaping the international system going forward in major ways." This sentiment was underscored in the remarks by Mike Brown, director of the U.S. Defense Innovation Unit, who noted, "If you are not leading on technology you lack authority in the governance realm." Democratic governments should prioritize R&D investment to sustain global competitiveness.

5) Democratic governments should make investments in civil society and efforts to strengthen democratic institutions. Civil society organizations have a role to play in promoting government accountability to rights-respecting digital practices, as well as in strengthening the resilience of communities through efforts to promote digital literacy and greater awareness of digital risks.

AUTHOR

Kip Wainscott is a Senior Advisor for the Global Digital Policy Incubator. A lawyer and policy professional with experience in government, civil society, and the private sector, he has worked extensively on issues concerning technology's impact on democracy and human rights.

*With research assistance from Catherine Baron and Tracy Navichoque.

This snapshot was created in partnership with the International Center for Not-for-Profit Law.

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW