Editor’s Note: This is the first article in a series on digital authoritarianism. The concept for the series emerged from a policy workshop hosted by Bridging the Gap and the Center for New American Security.
From Chinese government surveillance in Hong Kong and Xinjiang to Russia’s sovereign internet law and concerns about foreign operatives hacking the 2020 elections, digital technologies are changing global politics — and the United States is not ready to compete. As a first step, U.S. government officials need to understand how authoritarian regimes are using these tools to control their populations and disrupt democratic societies around the world. To this end, Bridging the Gap and the Center for a New American Security brought together a community of researchers and policymakers to address these questions. Participants included experts from Congress, the State Department, the National Security Council, and elsewhere in the U.S. government and the broader policy community, as well as outside scholars who prepared research-based memoranda for discussion. This introductory article kicks off a short series on this important topic that includes articles adapted from a selection of these memos.

While democrats once believed that innovations in information and communications technology and data analysis would promote more open societies, the actual effects of these tools have been mixed. Authoritarians are using technology to deepen their grip internally, spread propaganda, undermine basic human rights, promote illiberal practices beyond their borders, and erode public trust in open societies. Today, Russia continues its campaign of cyber and information attacks against democratic institutions and social cohesion in the United States and Europe. Iran and North Korea are following suit. The Chinese Communist Party is forging a future of mass surveillance and “social credit” scores, and rapidly exporting those tools to other parts of the world. Autocratic governments seem to be outpacing free societies in harnessing new technologies to advance their political goals.
The United States and like-minded countries must develop a new strategic framework to combat the rise of high-tech illiberalism. Building the right policy toolkit will require a deeper understanding of the strategic goals being pursued by authoritarian governments in the digital era — both within their borders and internationally — and of the methods these governments are employing in pursuit of these goals.

So far, U.S. policy responses to digital authoritarianism have been limited by several factors.

First, the U.S. government doesn’t understand technology very well. Yes, many foundations of the information economy were created through government initiatives, and advanced digital tools are employed throughout the government, especially in the national security community. But in the places where policy is made — Congress, the White House, and the political strata of cabinet agencies — politicians continue to apply old rules to new tools, hindering effective planning and responses.

Congress in particular has taken a “do-no-harm” approach to regulating technology companies — meaning no harm to corporate interests and innovation. The current model has led to a tech ecosystem in Silicon Valley and beyond that remains committed to Facebook’s old informal motto, “move fast and break things.” As a result, today’s digital marketplace generates new tools and platforms more rapidly than even industry experts can process.

Consider facial recognition technology, which has broad implications for how governments and others can surveil citizens. The unregulated nature of facial recognition tools has led technologists such as Microsoft president Brad Smith to practically beg for the government to step in. So far, such calls have been in vain. And if Congress can’t decide how to treat new technologies at home, it has little standing to call out wavering democracies or autocrats using these same tools overseas. Moreover, if the United States hopes to shape the future use of these
technologies, it must have a political and legal framework in place that other countries want to replicate. Without congressional action, this is unlikely to happen.

It’s a similar story with efforts to stop the manipulation of social media for political purposes. In the United States, policy on digital media content is governed largely by section 230 of the Communications Decency Act, which says that “interactive computer services” are in most cases to be treated as distributors of content, rather than as publishers. This has allowed platforms such as Facebook and Twitter to adopt a minimalist approach to moderating user content. (Like Microsoft’s Smith, Facebook founder and CEO Mark Zuckerberg has also called for more government regulation, but critics doubt the seriousness of his proposals.) Lax moderation has contributed to the well-publicized political exploitation of Facebook by Russian agents — which has continued in earnest since the 2016 election — and to the spread of hateful rhetoric that has led to riots and other violence in India and other countries around the world. New advances in “deepfakes,” facial recognition, and artificial intelligence, paired with rapid global technology adoption, will only intensify and accelerate these practices.

Second, evaluating the impact of even ostensibly benign technology depends on one’s perspective. While American corporations use data harvesting and analytics to micro-target consumer preferences, these algorithmic tools are equally being deployed to tailor disinformation for susceptible audiences in ways that pollute democratic discourse and threaten national security. New digital technologies that improve service delivery and public goods provision around the world can also be used in the service of public evils like targeted censorship and repression, which are often more effective at the subnational level. Steven Feldstein explores this dynamic in a subsequent article in this series. For example, policing tools such as China’s widely exported surveillance technology can promote not only necessary security but also authoritarianism in adopting countries.
Third, a surprising lack of U.S. competitiveness in the information and communications technology marketplace has ceded advantage to China and others. This stems in part from the ongoing wariness in the relationship between Big Tech and the U.S. government, and the lack of strategic alignment in American corporate and national interests abroad. Meanwhile, as Jessica Chen Weiss outlines in her forthcoming contribution to the series, Beijing has encouraged and paved the way for enormous Chinese corporate buildout overseas, with the spread of technology enabled by public–private partnerships to finance and build the supporting groundwork. The resulting digital infrastructure has embedded Chinese influence in key countries and regions for the foreseeable future. Huawei’s aggressive push to dominate global 5G wireless networks is a case in point. Whether or not this constitutes a sustained strategic campaign on China’s part, the cumulative effects of the diffusion of Chinese technology will have serious consequences for U.S. influence around the world.

The United States should take several steps to counter digital authoritarianism. First, it should improve regulatory practices to forestall the worst effects of digital technologies both at home and abroad. For Congress, this includes revisiting section 230 to promote more responsible approaches to moderating content, and encouraging platforms to shut down the authoritarian social media tactics, such as flooding and filtering, that Seva Gunitsky discusses in his forthcoming article in the series. Policymakers should also consider additional export controls on made-in-America tools that can be used for surveillance and political disruption, such as the restrictions recently imposed on China for its treatment of the Uyghur minority.

Externally, the United States should address the demand for illiberal surveillance technologies. In many cases, surveillance technologies are adopted to meet genuine local needs, such as reducing high crime rates. The U.S. government should identify those countries and localities most likely to import these technologies, and work to shape the policy landscape and legal frameworks that guide the use of technology
in these settings. This approach would leverage diplomacy and foreign aid to promote responsible adoption of digital technologies, including advising governments on how to protect privacy and civil rights as these tools are deployed, and developing alternative tools to compete with those currently in the marketplace.

Over the longer term, the United States will need to work with allies and partners to develop global standards for the use of surveillance and other potentially illiberal technologies. Establishing an overarching framework — akin to the arms control regime — that creates restrictions on the proliferation and use of new technologies would further enhance the resilience of democracy in the face of technological change. Such an agreement might also include provisions to sanction those who attempt to use digital technologies to disrupt democratic processes abroad, as the United States did following Russian efforts to interfere in the 2016 presidential and 2018 midterm elections. Recent research shows that such sanctions can be effective at signaling U.S. resolve and deterring future behavior, but are less useful for ending current practices. This highlights the need for a proactive rather than reactive sanctions approach, to make bad actors think twice before engaging in future illiberal practices.

Finally, policymakers and scholars concerned about digital authoritarianism ought to commit to further research and dialogue on the topic. This might include tripartite working groups convening policymakers, academics, and corporate actors to share information about the sources and types of technologies used by autocratic governments for surveillance, control, economic development, and public service provision. New research should also address how these tools are spreading across borders — in particular, how exporting countries such as China and Russia are helping other autocracies build internal digital infrastructures, what factors influence the ability and willingness of other countries to effectively use these technologies, and how societies across the world respond to authoritarian surveillance measures. We also need a clearer idea of how U.S.-based
companies are contributing to the abuses of digital autocracies around the world. The United States is losing ground in the race to leverage digital technologies to promote its national interests and values around the world. To meet this challenge, we need to understand it better.

BECOME A MEMBER

Naazneen Barma is associate professor of national security affairs at the Naval Postgraduate School, co-director of Bridging the Gap, and a 2019–2020 Berggruen fellow. She is author of The Peacebuilding Puzzle and her research centers on global governance and international engagement in post-conflict and developing countries.

Brent Durbin is associate professor of government at Smith College, co-director of Bridging the Gap, and a 2019–2020 Berggruen fellow. He is author of The CIA and the Politics of U.S. Intelligence Reform. His current research focuses on the political and social effects of new data technologies.

Andrea Kendall-Taylor is a senior fellow and director of the Transatlantic Security Program at the Center for a New American Security. She is a co-author of Democracies and Authoritarian Regimes. Her research focuses on Russia, authoritarianism, and national security challenges facing the United States and Europe.

Image: Pexels