THE CUTTING EDGE OF SHARP POWER

Christopher Walker, Shanthi Kalathil, and Jessica Ludwig

***Christopher Walker** is vice-president for studies and analysis at the National Endowment for Democracy (NED). **Shanthi Kalathil** is senior director of NED's International Forum for Democratic Studies, where **Jessica Ludwig** is a senior program officer.*

The pages of Wikipedia, sometimes referred to as the "world's encyclopedia," are consulted by users roughly twenty-billion times per month.[1] This popular online resource has arguably become a definitive global information gateway: Search-engine algorithms regularly place Wikipedia entries at the top of their lists of results, which also makes Wikipedia the chief source of replies to all manner of queries by Apple's "Siri" and other voice-assistant software. Wikipedia—launched in January 2001—is a prime example of the remarkable technological innovations that emerged at the turn of the twenty-first century. As a contributor-based platform open to a global audience, it relies on trust, cooperation, and transparency in the production of its content.

For all these reasons, the revelation in an October 2019 BBC report that more than a thousand "tendentious edits" had been made across nearly two-dozen sensitive articles relating to China shook the information platform. Mandarin-language entries had been rewritten to cast the 1989 Tiananmen Square massacre as "'the June 4th incident' to 'quell the counterrevolutionary riots.'" Taiwan—previously described as "a state in East Asia"—was redefined as "a province in the People's Republic of China." Other edits similarly sought to reframe matters past and present in a manner congenial to the ruling Chinese Communist Party (CCP). The BBC concluded that, while the source of the edits could not be proven, "there are indications that they are not all necessarily organic, nor random." It highlighted calls by People's Republic of China (PRC) experts and by an official from a party-controlled publishing body for action to change the tenor of Wikipedia entries.[2] Wikipedia, it bears noting, is currently blocked for ordinary users in the PRC.

Journal of Democracy Volume 31, Number 1 January 2020

The hand of the CCP regime was more clearly visible in the October 2019 controversy that followed a stray tweet from Daryl Morey, general manager of basketball's Houston Rockets, concerning recent mass protests in Hong Kong. Since March 2019, demonstrators—initially protesting a new extradition law and later voicing concerns about police violence and eroding democratic liberties—have taken to the streets in actions that have drawn millions in a territory of fewer than eight-million people. Morey's brief tweet supporting the protests drew an initial outpouring of state-led online condemnation in the PRC,[3] with China's basketball association, state and online media, and corporate sponsors eventually cutting their cooperation with the Rockets and with the U.S. National Basketball Association (NBA) more broadly. Statements by NBA players and officials distancing themselves from Morey touched off a firestorm of public debate. Subsequent analysis indicated that Morey was the target of an online troll attack intended to manipulate the conversation about the Hong Kong protests.[4]

The Authoritarians' Outward Turn

These efforts to control online discourse are part of a larger challenge that has taken shape in an era of resurgent and globalized authoritarianism. Manipulation of information at its source and a wider offensive by antidemocratic powers in the realm of ideas have challenged some deeply held assumptions in democratic polities. One of these assumptions was that, if democracies engaged patiently with authoritarian states, both sides would unambiguously benefit.

China offers the most striking illustration of this emerging pattern, although it is far from the only such case. In the three decades since the Tiananmen Square crackdown, Western decision makers and experts have overwhelmingly viewed China through an economic-development lens. It is only quite recently that the general policy community—prompted in part by China's heavy-handed pressure on the NBA—has begun to overcome the blind spot that resulted from this narrow framing. A more multidimensional view of the modern Chinese party-state is now gradually coming into focus as analysts start taking into account China's global impact on democracy, rule-of-law norms, and human rights, including the freedom of expression.

The democracies' decision to engage with China unconditionally—rather than in a principled manner—has yielded worrisome results. The CCP, far from embracing political reform, has progressively tightened its authoritarian grip. Moreover, Beijing is expanding its repressive practices outward and increasingly harnessing new technologies to spread its values and its vision for the world. Although China today is heavily interconnected with the international system, it has not become more transparent and accountable. Instead, the CCP has striven to re-

shape the global landscape in a manner that suits its preferences—and it has not been alone in these endeavors. Moscow, the Gulf States, and other leading authoritarian regimes have likewise developed outward-facing policies and practices that are corroding democratic standards.

The resulting challenge is formidable not least due to the sheer geographic reach of today's activist autocrats. In the Horn of Africa, Russia, China, and several Gulf states are vying for influence in ways that are plainly inhospitable to democratic development and human rights. Saudi Arabia wields prodigious influence in Southeast Asia, among other places, in spheres (such as media and technology) that are central to democratic development. In the Balkans, a constellation of authoritarian powers is at work, often leveraging the efforts of like-minded local forces to hinder or reverse the emergence of more accountable and transparent governance.[5] Similar scenes are playing out in Latin America and elsewhere. Russia and China are wielding their influence in systems of all types, including those of the United States and other advanced democracies.

Analysts were not expecting things to turn out this way. Writing in 1990, Dankwart Rustow captured the spirit of the times by stressing "the global trend of intensifying communication and economic integration": "Whereas democracies have thrived amid this flood of messages and goods," he observed, "dictatorships had difficulty isolating themselves from it."[6] It was hard to foresee just how profoundly the next phase of the communications and technological revolution would alter the global political landscape.

Although it has only recently begun to attract widespread attention, the global authoritarian resurgence did not emerge overnight. By the early 2000s, the autocrats were already rebuilding their capacity to exert influence. Leading authoritarian powers have over the years made calculated investments in the ideas realm, including support for think tanks, people-to-people exchanges, and initiatives in the fields of diplomacy, education, media, and technology. These efforts laid the groundwork for a new era of competition that is placing the world's democracies in an unexpectedly precarious position.

This longstanding investment has paid particularly large dividends in the technological domain. Samantha Hoffman, describing China's use of technology "to augment its authoritarianism," notes that "what we are seeing now is a manifestation of plans already in place and in fact public for years, even decades. We are still underestimating their potential."[7] The same could be said of other authoritarian regimes. Vladimir Putin's Russia has insistently channeled to its swollen state-security apparatus and global influence machine resources that might have gone to the country's underfunded schools and hospitals.

The authorities in Beijing and Moscow develop strategies of information and political manipulation at the domestic level and then test and

apply them beyond their national borders. Russia's much-noted media-manipulation infrastructure, which spans the realms of traditional and social media, was designed for maintaining domestic control but has been adapted for international application. The infamous St. Petersburg–based "Internet Research Agency," widely known for its corrosive activities in U.S. and other foreign election campaigns, has as its main task trolling the Putin regime's opponents within Russia.[8]

China's influence activities appear to be following a similar path. Manipulation tactics employed within mainland China now also make up one facet of Beijing's ever more intrusive approach to Hong Kong and Taiwan. The PRC's paid internet trolls are believed to be behind a barrage of misleading online political content that was directed at Taiwanese citizens via Twitter, Facebook, and chat groups during the run-up to Taiwan's November 2018 elections.[9] And Russia and China, while particularly prominent, are far from the only authoritarian actors expanding the frontiers of digital deception: Facebook has linked Saudi Arabia, for instance, to the creation of hundreds of recently banned accounts and pages that presented themselves as belonging to citizens or news outlets in various Middle Eastern and North African countries.[10]

Understanding Sharp Power

In 2017, a *Financial Times* article offered some unsolicited advice for the architects of China's influence activities: In its "efforts to build soft power outside its borders . . . [China] needs to tread more lightly, and take a more reciprocal and less authoritarian approach."[11] But this sensible exhortation raises a key question: Why would a regime that monopolizes power and brooks no dissent at home choose to operate differently beyond its borders? While authoritarians have excelled at exerting influence in an increasingly interconnected world, their activities are a poor fit for the categories that predominated in the Cold War's aftermath. The concept of "soft power"—the "ability to affect others by attraction and persuasion"[12]—often fails to capture what goes on when autocrats reach abroad. We have argued that these efforts instead represent the exercise of "sharp power," which seeks to impair free expression, to compromise and neutralize independent institutions, and to distort the political environment.[13]

The compromising effects of sharp power are today visible in many spheres. The authoritarians' refined and expanded activities threaten the integrity of institutions from media and entertainment companies to universities to professional sports enterprises—all of which are vulnerable to manipulation precisely because, in free societies, such institutions are open to the outside world.[14] Universities and publishers face legal, financial, and administrative pressures that threaten to stifle discussion on topics that bruise authoritarian sensitivities. It is becoming increasingly

clear that capital and investment flows from authoritarian sources bring with them discourse-stifling "noneconomic costs" of this sort, which can impinge on the integrity of democratic institutions. In the media and technology domains, authoritarians are investing massive resources to attain a leading position in global markets—and in the process they are changing how people around the world perceive facts and engage with technology.

Leaders in Beijing and Moscow aim to gain control over the tools for disseminating information, images, and ideas. These regimes are expanding not only their media footprint, visible in the form of state-run international broadcasters such as RT and CGTN, but also their efforts at manipulation and censorship. The aim of these autocracies is to make information available in a selective way, something that is both integral to censorship and a key attribute of sharp power. As Russia and China enhance both their information activities and their technological capacity in fields such as artificial intelligence (AI) that are key to manipulating public perceptions, their ability to curate information flows—especially in places where local media organizations are vulnerable—is likely to continue to grow.

In his 1990 essay, Rustow described a landscape in which "the worldwide revolution of technology, communications and travel . . . not only spread the awareness of democratic life-styles, but also helped expose th[e] hypocrisy of 'democracy' in communist and Third World countries." Today, the autocrats have turned the tables. The Kremlin's global influence machine is emblematic of this trend: It seeks to blur perceptions of the corruption and hypocrisy that pervade Russia's repressive system, while polluting public discourse in democracies so as to undermine the health and credibility of these regimes. From Australia to Austria to Argentina, democracies must reckon with authoritarians who are working to reshape the international environment. To make matters even more difficult, all this is occurring while established democracies are distracted by their own internal struggles. These developments should be of deep concern to all who value accountable governance and human rights.

When it comes to the impact of authoritarian sharp power on the future of democracy, perhaps no other domain is as pivotal as that of technology. In the digital realm, sharp power is keenly felt yet often not perceived as such. Authoritarian success at exploiting the technological revolution has caught the democracies by surprise: Since the days of smuggled cassettes bringing banned voices to listeners in the Soviet Union, technology has been widely seen as tied to the cause of freedom. The libertarian ethos that permeated early Silicon Valley bolstered these perceptions. As the internet and related technologies spread rapidly in the early twenty-first century, many assumed that authoritarian regimes would be unable to manage their political impact.[15] Conventional wisdom held that the diffusion of information technology would open up

closed political space, while also transmitting and reinforcing democratic norms. As the information revolution advanced into the age of social media and machine learning, ever deeper forms of technological interdependence between democracies and authoritarian regimes emerged.

In many important ways, new technology did foster freer information flows in authoritarian countries, enabling forms of expression, mobilization, and improved governance that should not be dismissed. But in the afterglow of the immediate post–Cold War period, democracies failed to foresee the dark side of technological interdependence—namely, that it would enable modernizing authoritarians to reach across borders to censor and manipulate public discourse, sharpen polarization, and undermine democracy.

The Technological Revolution

Today's ubiquitous instant-communications tools have opened up unexpected avenues for the manipulation of public opinion, political processes, and democratic institutions. Digitally connected citizens are increasingly getting their news from social-media platforms, yet there is evidence that the algorithms that drive these platforms are interacting with users' emotions and cognitive biases in ways that facilitate the spread of misleading content.[16] This combination has fed growing mistrust in traditional information outlets and governance institutions. While illiberal actors within democracies undoubtedly use tactics that exploit and deepen this mistrust, internationalist authoritarian regimes stand out for the massive resources they have dedicated to these aims. Democracies are largely navigating these challenges haphazardly as they arise—and democratic governments are even less prepared to traverse the still-rockier landscape that looms over the horizon.

Although the authoritarians' influence activities are sometimes discussed under the rubric of "exporting authoritarianism," autocrats do not simply hand over a blueprint for digital authoritarianism to a small club of eager dictators. Technology shaped by authoritarian values has also found purchase within open societies around the world. "Safe-city" surveillance projects peddled by the Chinese telecommunications giant Huawei can be found in municipalities in Germany, Italy, the Netherlands, and Spain.[17] The Kremlin's use of disinformation to sow distrust in democracy has furnished an adaptable model that both state and nonstate actors can follow. In addition, technology is enhancing authoritarians' ability to surveil and pressure opponents who have found refuge abroad: For example, critics of the Saudi and United Arab Emirates regimes based in Canada and the United Kingdom have been targeted with high-end spyware programs in what experts believe are likely state-linked attacks.[18] The Chinese party-state also uses sophisticated technology to surveil and threaten Uyghurs, Tibetans, and others who are living outside China's borders.

Until democracies were forced to confront the fallout of authoritarian intervention in their own politics, few imagined that authoritarians would be so successful at manipulating dominant social-media platforms through computational propaganda (which draws on algorithms, automation, and big data to aim content at receptive audiences). Similarly, the authoritarian-conceived norm of "cybersovereignty," in which national borders partition the internet and curtail or even halt the free flow of information, used to be dismissed as a dictator's pipe dream. Now tech titans and opinion leaders almost take for granted a splintered internet that essentially hews to this vision, with access for citizens of authoritarian regimes curtailed by censorship, surveillance, internet shutdowns, and the like. Russia's recent enactment of a "sovereign internet law" that will facilitate site-blocking and shutdowns is only the latest chapter in the evolution of this norm. The counternarrative has become the narrative.

All this has come about thanks to the considerable effort that authoritarian regimes have made to shape the technological environment—including platforms, hardware, software, standards, and architecture, as well as norms and conceptual framing. At a recent high-level summit that brought African leaders to Sochi, for instance, a representative of Russia's defense-export agency touted the facial-recognition systems on offer as "the most precise in the world." Clients in Latin America, the Middle East, and especially postcommunist Eurasia are patronizing Russian IT companies whose offerings include surveillance options on the model of Russia's SORM system (which provides authorities with copies of all internet traffic).[19]

The CCP has been forging an increasingly seamless synthesis combining consumer convenience, surveillance, and censorship. This model is exemplified by such all-encompassing platforms as WeChat, which combines messaging, online-payment, and many other functions. Everyday life in China, particularly for younger people, is increasingly dependent upon this app, which includes politically based content restrictions and lends itself to surveillance (for instance, through selectively required user "faceprints").[20] Now prevalent within China, this tech model is increasingly being packaged for foreign audiences as part of the CCP's signature foreign-policy project, the Belt and Road Initiative.

The CCP's technological innovations have contributed to some of the world's worst human-rights abuses—including the incarceration and surveillance of millions of ethnic Uyghurs in China's Xinjiang region. Western researchers and technology firms, wittingly or not, have supplied the know-how, capital, and investment that have enabled the CCP to pen a litany of dystopian horror stories, from DNA harvesting to police apps that track people's most mundane activities.

Yet China and other autocracies cannot simply will into existence overseas replicas of their surveillance states. How technologies get used around the world depends on the populations that interact with them,

the democratic and rights-based safeguards put in place by individual societies, and the democracies' success at defining and defending their values within international institutions. Strong democratic safeguards that protect the rights of the vulnerable are essential. Even if the authoritarian behemoths do not explicitly seek to remold the world in their own image, the dangers to civil liberties are growing as authoritarian styles of social management are being baked into the world's technological architecture (for instance, through SORM-enabled internet services or "smart-city" systems that enable regimes to track political opponents). When these technologies are adopted in places where civil society and government oversight are not robust, they may well facilitate the closing of civic space and the normalization of authoritarian values.

Even if the authoritarian behemoths do not explicitly seek to remold the world in their own image, the dangers to civil liberties are growing as authoritarian styles of social management are being baked into the world's technological architecture.

Authoritarian regimes are working to shape the international standards and norms that will affect how the next generation of technology is conceptualized, put into use, and received around the world. Russia, for instance, has used intergovernmental forums and treaty proposals to promote a definition of cybersecurity that includes not only protection against hacking, but also control over information dissemination in a state's "sovereign" cyberspace.[21] Simply nudging debates about the values that should govern new technologies away from international human-rights standards can help authoritarian regimes to legitimize the use of technology for repression.

These issues are particularly crucial given the accelerating pace of technological change. New frontiers in surveillance have opened up due to advances in machine learning (a process whereby programs are trained to process large volumes of data, identify patterns, and draw conclusions in a way that imitates intelligent human behavior), which powers technologies from facial recognition to predictive tools used in criminal justice. These advances enable authorities to surveil using not only cameras and spyware, but also the millions of recordable data points that people "opt" to emit simply by carrying out everyday activities such as shopping online, updating social-media accounts, or joining a consumer-rewards program. The full realization of the Internet of Things (networked everyday objects) poses an even more vexing conundrum: How will future democratic activists guard themselves against a battalion of data-sucking vacuum cleaners (which also map floor plans), heart monitors (which send information about physical and emotional

changes), and smart speakers (which sense and record voice information), all of which might be sharing and combining the data they record under perfectly legal terms of service?

From these massive quantities of what experts call "data exhaust," private-sector and government actors alike will be able to reconstruct individuals' preferences, personalities, habits, and even medical conditions on a scale previously unimaginable. These vast data stores will also facilitate information campaigns ever more precisely targeted to capture people's attention and alter their thinking and behavior. Combined with the use of AI-powered video, voice, and sensory manipulation to produce so-called deep fakes that convince viewers they are witnessing events that never actually took place, this information microtargeting is likely to further erode any agreement across audiences on a shared notion of objective truth.

For those authoritarian states willing to keep investing in such endeavors, the possibilities for gaining asymmetrical advantages within the open public and civic space of democracies are vast—a fact not lost on the Chinese party-state, which has been engaging in massive data-collection efforts. When systems such as facial-recognition software, translation services, and data-visualization programs are provided by state-linked PRC firms and then used abroad, the party-state may gain access to the data these systems process. One major producer of these technologies is a subsidiary of a state-owned enterprise answerable to the CCP's Central Propaganda Department. In addition to whatever value such data hold in their own right, they can help PRC developers to refine technologies that monitor public sentiments, generate automated online comments, and otherwise facilitate "social management."[22] Savvy activists will always devise clever and often low-tech ways to avoid surveillance (such as the face masks used by the Hong Kong prodemocracy protesters), but over the long run the advantages may accrue to the authoritarians—absent a more purposeful response from the democracies.

Building Democratic Resilience

Antidemocratic powers, building on many years of material and political investment, have become adept at turning democratic societies' very openness against them—especially in the realm of technology. While Moscow and Beijing have worldviews that diverge in some ways, they share an approach that discourages pluralism, suppresses independent voices, and neuters accountability. Today, the distorting and compromising effects of authoritarian sharp power on the health of young and established democracies alike are increasingly evident.

Mounting an effective response will require creative thinking. A longer-term, more purposeful strategy rooted in civil society as well as in state institutions can help democracies to defend their security and

retake the initiative over the longer term. Such a response must reinforce, at the most fundamental level, the democratic principles it seeks to protect. It should focus on the following goals:

Reinforcing democratic principles: Authoritarian powers seek to corrode the integrity of democratic institutions. Therefore, democratic societies must identify approaches that draw on their own strengths and that reinforce the integrity of civic institutions together with support for democratic principles. The drastically increased scale of authoritarian efforts at manipulation and censorship presents a qualitatively new challenge for institutions in the spheres of publishing, education, culture, business, media, and technology. To guard against sharp power, the leaderships of these institutions must take concrete steps toward renewing their commitments to democratic standards and free political expression. Identifying these standards can often be straightforward: Many of the institutions concerned are already formally committed by their charters or other public statements to such principles as transparency, accountability, and free expression.

Deepening democratic unity: At the same time, the mechanisms for deepening these commitments are not self-evident. They may require collective approaches. Authoritarian regimes employ divide-and-conquer methods that aim at isolating and subverting both individual democracies and institutions within them. Russian and Chinese leaders seek to divide allies within the trans-Atlantic community; within Europe, China has cultivated separate relations with the countries of Central and Eastern Europe through its "17+1" initiative. A similar pattern has been evident at the subnational level. Until now, it has been far too easy for the institutions of civil society to be isolated and picked off one by one. These independent institutions must take the initiative to develop and defend common standards. One illustrative response is a 2018 statement by the Association of University Presses, which reaffirms guiding principles in the face of growing pressure from governments to censor access to specific content.[23]

Cultivating new expertise: In many open societies, a lack of expertise about resurgent authoritarian regimes has contributed to an underestimation of the challenge. This represents a crucial strategic gap for countries that are struggling to cope with their growing engagement with well-resourced authoritarian powers. Democratic policy makers need expert knowledge about the regime-survival incentives that drive autocracies and about the relationship between these regimes and their nominally autonomous private-sector or "nongovernmental" actors. To this end, it is crucial that both established and younger democracies develop an independent capacity to monitor and analyze local engage-

ment with authoritarians. The difference that such expertise makes is illustrated by the case of Australia, where increased media reporting, think-tank analysis, and academic research are contributing to a serious public debate about CCP influence.[24]

The intent of sharp power is to obscure. In the absence of expert monitoring and analysis, it hums quietly along in the background. Viewed in isolation, any one of the various media initiatives that Beijing supports—sponsored editorial inserts in foreign newspapers, content-exchange agreements, "trainings" in China for foreign journalists, or state-media broadcasts aimed at foreign audiences—may appear innocuous. Yet taken together, they signal an intent to manipulate global discourse regarding China's authoritarian system, suppressing and crowding out discussion of issues that the CCP would rather see ignored. The digital disinformation tactics honed by Russia muddy the waters of democratic debate by convincing targets that they are interacting with their fellow citizens, not foreign trolls. Developing effective democratic resilience will require journalists, civil society organizations, and country and subject-matter experts, including those who possess specialized tech-related acumen, to work together, and across borders.

Meeting the technology challenge: The invasive forms of technology widely adopted in recent years tend to favor authoritarian values and practices.[25] The desire for increased connectivity is strong everywhere, but especially so in developing economies seeking to increase their low internet penetration rates and to stimulate economic growth. Thus when China and other authoritarian regimes offer to facilitate access to new technology infrastructure, equipment, and software, the recipient countries are sometimes willing to overlook the political risks of closer engagement.

A crucial factor in this equation is the lack of debate in authoritarian settings about the norms governing tech usage and development. This does not mean that technologies produced in democracies are inherently conducive to free expression, transparency, and other democratic values; current debates show that this is far from the case. Yet the very existence in open societies of vigorous debate and accountability mechanisms can have an impact. This was evident in two recent incidents: the outcry that followed a whistleblower's revelation of Google's work on a censored version of its search platform for use in China; and the decision by officials in San Francisco to ban any local-government use of facial-recognition technology that has not undergone formal review, approval, and public disclosure.[26]

In authoritarian systems, by contrast, little that affects the government's strategic interests takes place independent of official guidance. Initiatives in the technology sphere generally are state-funded or are given strong incentives to cooperate with the authorities. In the absence of independent

civil societies, authoritarian technological development is subject to minimal oversight and little pressure to safeguard the rights of the vulnerable. When platforms developed in these settings spread to democratic countries, authoritarian political norms may come along for the ride. In September 2019, for instance, leaked documents revealed that the Chinese-owned social network TikTok—a globally popular service designed for sharing user-created videos—had told its moderators to censor videos mentioning Tiananmen Square, Tibetan independence, and other subjects considered sensitive by the Chinese government.[27] Experts and policy makers in democratic societies face the dual challenge of addressing the spread of technology developed in authoritarian settings while also ensuring that platforms based in democratic countries uphold democratic norms.

Democratic societies face the dual challenge of addressing the spread of technology developed in authoritarian settings while also ensuring that platforms based in democratic countries uphold democratic norms.

Democracies have been slow to realize that the diffusion of technology does not automatically foster freer information flows and democratic practices; policies and norms must be deliberately crafted with these outcomes in mind. Civil society can help to fill the gap and stimulate public debate by shining a light on how imported authoritarian technologies are used. The work of local civil society organizations informed international reporting on Ecuador's ECU 911 surveillance-camera monitoring network, which was funded through a loan from Beijing and built by Huawei and a Chinese state-owned enterprise. Although this network was purportedly a tool for policing and humanitarian response, a *New York Times* investigation disclosed that Ecuador's intelligence agency also has access to camera footage.[28] As similar surveillance networks proliferate in other countries as part of public-security and smart-city initiatives, civil society organizations can learn from such examples in thinking about how to monitor them.

If authoritarian standards become more widely embedded, the space for independent information will continue to shrink, weakening the health of democracy where it already exists and hobbling prospects for democratic advances elsewhere. To set things on a more positive course, democracies must set the standard for accountability, transparency, and human-rights protection. This effort must involve not only governments, but also the institutions of civil society that give democracies their lifeblood and resilience.

Democracies need to articulate a comprehensive, coherent, and collective vision that takes a clear-eyed view of the challenges posed by the modern information ecosystem and establishes a principled framework for responding to them. Such a framework must include innovations that

enable democrats to take greater advantage of technological advances. Open democratic societies have a key strategic advantage that closed authoritarian systems lack—the creativity and initiative of vibrant, pluralistic civil societies that can inform, support, and help to realize such a vision. Democratic systems must draw upon the full range of their capabilities if they are to meet the many-faceted authoritarian challenge.

NOTES

1. Recent page-view statistics may be found at *https://stats.wikimedia.org/v2/#/all-projects/reading/total-page-views/normal|bar|2-year|~total|monthly*.

2. Carl Miller, "China and Taiwan Clash over Wikipedia Edits," BBC, 5 October 2019, *www.bbc.com/news/technology-49921173*.

3. Sarah Cook, "State-Led Content Manipulation Drove the Backlash Against the NBA in China," Freedom House, *Freedom at Issue* blog, 13 November 2019, *https://freedomhouse.org/blog/state-led-content-manipulation-drove-backlash-against-nba-china*.

4. Ben Cohen, Georgia Wells, and Tom McGinty, "How One Tweet Turned Pro-China Trolls Against the NBA," *Wall Street Journal,* 16 October 2019, *www.wsj.com/articles/how-one-tweet-turned-pro-china-trolls-against-the-nba-11571238943*.

5. Kurt Bassuener, "Pushing on an Open Door: Foreign Authoritarian Influence in the Western Balkans," International Forum for Democratic Studies, National Endowment for Democracy, May 2019, *www.ned.org/wp-content/uploads/2019/05/Pushing-on-an-Open-Door-Foreign-Authoritarian-Influence-in-the-Western-Balkans-Kurt-Bassuener-May-2019.pdf*.

6. Dankwart A. Rustow, "Democracy: A Global Revolution?" *Foreign Affairs* 69 (Fall 1990), *www.foreignaffairs.com/articles/1990-09-01/democracy-global-revolution*.

7. Samantha Hoffman, "China's Tech-Enhanced Authoritarianism," Testimony Before the House Permanent Select Committee on Intelligence, Hearing on "China's Digital Authoritarianism: Surveillance, Influence, and Political Control," 16 May 2019, *https://docs.house.gov/meetings/IG/IG00/20190516/109462/HHRG-116-IG00-Wstate-HoffmanS-20190516.pdf*.

8. Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality* (New York: PublicAffairs, 2019), 18–21.

9. Josh Rogin, "China's Interference in the 2018 Elections Succeeded—in Taiwan," *Washington Post,* 18 December 2018, *www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan*.

10. Jack Stubbs, "Facebook Says It Dismantles Covert Influence Campaign Tied to Saudi Government," Reuters, 1 August 2019.

11. "China's Soft Power Comes with a Very Hard Edge," *Financial Times,* 2 November 2017.

12. Joseph S. Nye, Jr., "China's Soft and Sharp Power," *Project Syndicate,* 4 January 2018, *www.project-syndicate.org/commentary/china-soft-and-sharp-power-by-joseph-s--nye-2018-01?barrier=accesspaylog*.

13. See International Forum for Democratic Studies, *Sharp Power: Rising Authoritarian Influence* (Washington, D.C.: National Endowment for Democracy, 2017), 13, *www*.

ned.org/wp-content/uploads/2017/12/Introduction-Sharp-Power-Rising-Authoritarian-Influence.pdf; Christopher Walker, Shanthi Kalathil, and Jessica Ludwig, "How Democracies Can Fight Authoritarian Sharp Power," *Foreign Affairs,* 16 August 2018; Christopher Walker, "What Is 'Sharp Power'?" *Journal of Democracy* 29 (July 2018): 9–23.

14. Walker, Kalathil, and Ludwig, "How Democracies Can Fight."

15. Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, D.C.: Carnegie Endowment, 2003).

16. Dean Jackson, "Issue Brief: The 'Demand Side' of the Disinformation Crisis," National Endowment for Democracy, 2 August 2018, *www.ned.org/issue-brief-the-demand-side-of-the-disinformation-crisis*.

17. Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, 17 September 2019, *https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847*.

18. Bill Marczak et al., "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *Citizen Lab,* 1 October 2018, *https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil*; Bill Marczak and John Scott-Railton, "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents," *Citizen Lab,* 29 May 2016, *https://citizenlab.ca/2016/05/stealth-falcon*.

19. AFP, "Guns and Smiles: Russia Flaunts Firepower at Africa Summit," News 24 (South Africa), 24 October 2019, *www.news24.com/Africa/News/guns-and-smiles-russia-flaunts-firepower-at-africa-summit-20191024-2*; Robert Morgus, "The Spread of Russia's Digital Authoritarianism," in Nicholas D. Wright, ed., *Artificial Intelligence, China, Russia, and the Global Order* (Maxwell Air Force Base, Ala.: Air University Press, 2019), 95.

20. Stephen McDonell, "China Social Media: WeChat and the Surveillance State," BBC, 7 June 2019.

21. Morgus, "The Spread of Russia's Digital Authoritarianism," 93.

22. Samantha Hoffman, *Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion* (Australian Strategic Policy Institute, 2019), *https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT*.

23. "Facing Censorship: A Statement of Guiding Principles," Association of University Presses, 21 March 2018, *www.aupresses.org/component/content/article/53-intellectual-freedom/1692-facing-censorship-a-statement-of-guiding-principles*.

24. Walker, Kalathil, and Ludwig, "How Democracies Can Fight."

25. Ronald J. Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media," *Journal of Democracy* 30 (January 2019): 25–39.

26. See Alex Hern, "Google Whistleblower Launches Project to Keep Tech Ethical," *Guardian,* 13 July 2019; Gregory Barber, "San Francisco Bans Agency Use of Facial-Recognition Tech," *Wired,* 14 May 2019.

27. Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *Guardian,* 25 September 2019. The company claimed to have since replaced these instructions with "localised approaches."

28. Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *New York Times*, 24 April 2019.