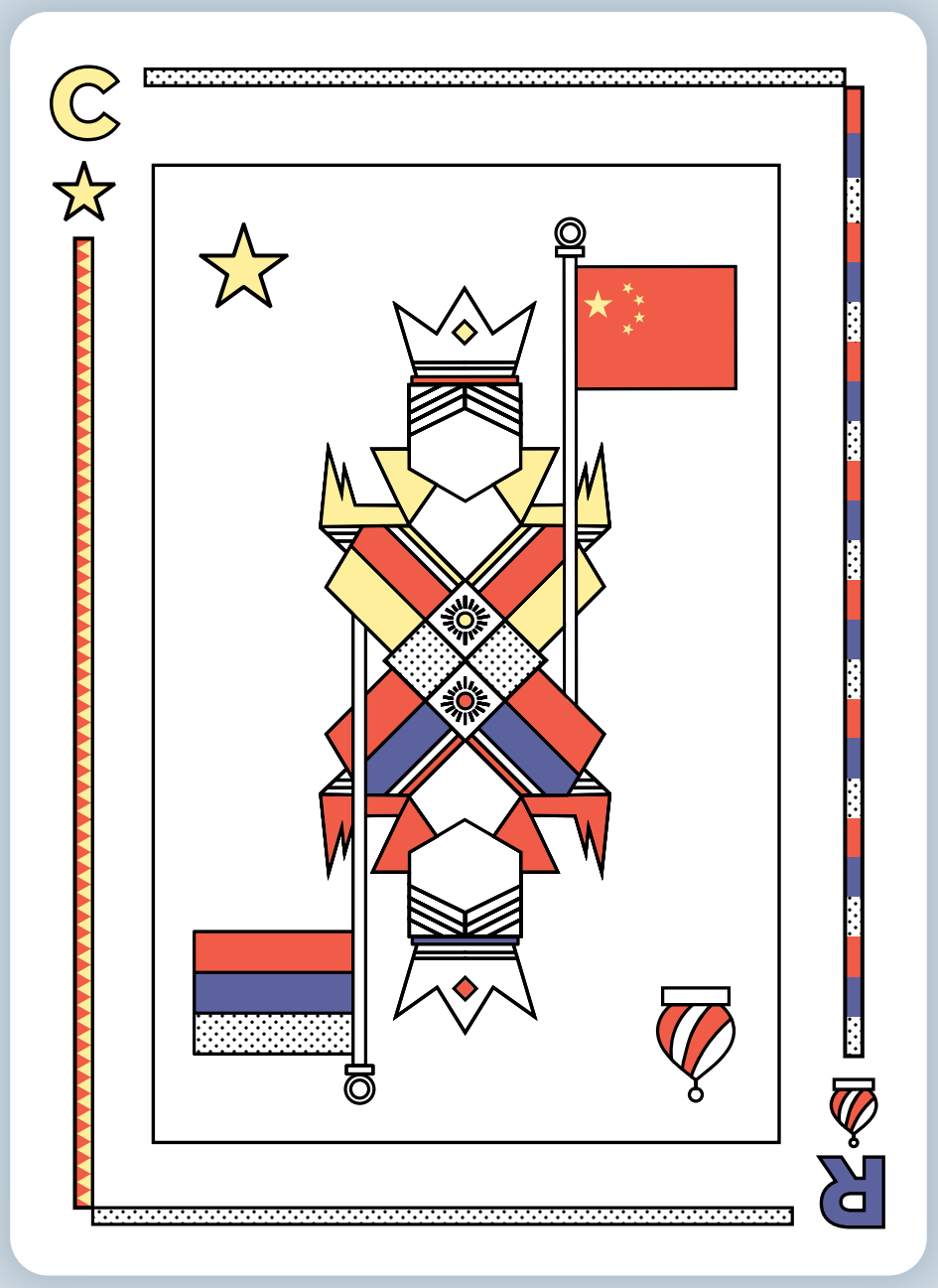
MAY 2020

Dangerous Synergies

Countering Chinese and Russian Digital Influence Operations

Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche



CNAS

About the Authors

Dr. Daniel Kliman is Senior Fellow and Director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS). He focuses on U.S. strategy toward China and on the future of U.S. alliances and partnerships in the Indo-Pacific. Before joining CNAS, Kliman worked in the U.S. Department of Defense, where he served as Senior Advisor for Asia Integration. His most recent book is *Fateful Transitions: How Democracies Manage Rising Powers, from the Eve of World War I to China's Ascendance* (University of Pennsylvania Press, 2014).

Dr. Andrea Kendall-Taylor is Senior Fellow and Director of the Transatlantic Security Program at the Center for a New American Security. She works on national security challenges facing the United States and Europe, focusing on Russia, authoritarianism and threats to democracy, and the state of the transatlantic alliance.

Kristine Lee is an Associate Fellow for the Asia-Pacific Security Program at the Center for a New American Security. She received her Bachelor of Arts from Harvard College, where she was editor-in-chief of the *Harvard International Review* and was awarded a Fulbright fellowship. She earned her Master in Public Policy from the Harvard Kennedy School, with a focus on international relations and security studies in the Asia-Pacific region.

Joshua Fitt is a Research Assistant for the Asia-Pacific Security Program at CNAS. He focuses on U.S. East Asian security strategy and specializes in Japanese and Korean Peninsular affairs. Before joining CNAS, Fitt was a campaign field organizer during the 2018 midterm elections in the Upper Midwest, an earthquake and tsunami disaster relief volunteer with IsraAID in Japan, and the Council on Foreign Relations' Japan Program Intern. He earned his BA in East Asian Studies from Yale University.

Carisa Nietsche is the Research Associate for the Transatlantic Security Program at the Center for a New American Security. She specializes in populism; European security; and threats to democracy in Europe, particularly in Hungary, Poland, and Turkey.

Acknowledgments

The authors are grateful to the many officials and experts who shared their perspectives during the course of the project through participation in roundtable meetings at CNAS. This report would not have been possible without assistance from a variety of current and former CNAS colleagues, including Karina Barbesino, Jasmine Butler, Melody Cook, David Dee, Chris Estep, Allison Francis, Shai Korman, Maura McCarthy, Dan McCormick, Ely Ratner, and Loren DeJonge Schulman. In addition, the authors would like to thank Laura Rosenberger for reviewing a full draft of this report. The views presented here are the authors' alone and do not represent those of CNAS or any other organization. The authors are solely responsible for any errors in fact, analysis, or omission.

TABLE OF CONTENTS

01 Executive Summary

03 Introduction

04 The Role of Digital Influence in the Foreign Policy Toolkits of China and Russia

06 Mutual Interests Driving Chinese and Russian Digital Influence Operations

07 Different but Converging Approaches to Digital Interference

11 Digital Influence Tools Used by China and Russia

16 How Chinese and Russian Digital Influence Efforts are Mutually Reinforcing

20 Forecasting China-Russia Synergies

24 Recommendations

27 Conclusion

Executive Summary

The 2016 U.S. presidential election and the 2018 and 2020 Taiwanese local and presidential elections crystallized that Russia and China are using digital interference to shape the contest between democracies and autocracies. While foreign information operations are time-tested methods of authoritarian influence, the digital space has increased the scope and speed with which these operations can be waged. Although there is no concrete evidence to suggest that Beijing and Moscow explicitly coordinate their information operations, the two countries are increasingly finding common cause as their interests align on a number of issues and in strategic regions.

Their digital influence campaigns work in tandem and toward the following objectives:

1. Undermine liberal democratic norms and institutions.
2. Weaken cohesion among democratic allies and partners.
3. Reduce U.S. global influence.
4. Advance Russian and Chinese positions.

Over the last several years, Beijing and Moscow have taken different paths to advance these shared goals. Although the differences in their approach to digital influence are likely to persist, there is growing evidence that the two countries are learning from each other and enhancing their coordination, leading to a growing convergence in their digital influence efforts. This is occurring in real time as China and Russia seek to obscure the origins of COVID-19 and while Beijing cynically recasts itself as the global leader in responding to the very pandemic it failed to contain.

Dangerous Synergies

Democracies worldwide are likely to see growing synergy between the two authoritarian powers in the information environment. In fact, digital influence efforts by China and Russia have already proved mutually reinforcing by:

Magnifying impact through complementary approaches. Although China's and Russia's approaches are different and seemingly uncoordinated, taken together, they have a more corrosive effect on democracy than either would have single-handedly.[1] Russia propagates narratives designed to undermine trust in institutions and elected governments, and this creates fertile ground for Chinese narratives about the superiority of authoritarian systems to take root.

Amplifying narratives. There are a growing number of instances in which Chinese and Russian narratives overlap, amplifying the impact of such messages. Chinese and Russian media and diplomatic institutions have forged symbiotic relationships that support the creation of an entirely alternative information ecosystem in which truth is called into question.

Legitimizing norm change. In multilateral forums, China and Russia are jointly chipping away at norms and standards governing the free flow of information. Together, they seek to bend the arc of the global information architecture to their advantage by legitimizing high-tech illiberalism at home while continuing to exploit the relative openness of the United States' and other democracies' digital environment.

The coordination and resulting synergy between China and Russia in the informational domain is likely to grow. Their expanding ties, including those related to digital influence, will provide a foundation for greater cooperation and coordination, increasing the challenges the United States and democracies globally will face. Looking forward, the United States and its democratic allies and partners should expect Beijing and Moscow to:

Deepen coordination. China and Russia already conduct a number of exchanges designed to share technologies and processes to control the internet. Beijing and Moscow could leverage their comparative strengths to pollute the global information environment while setting forth alternative platforms by which information can be disseminated.

Divide and conquer. While Russian efforts remain most intensely focused on weakening and dividing democratic societies in Europe and the United States, China is spreading the tentacles of its online influence campaigns in strategically positioned developing countries across Southeast Asia, Central Asia, Latin America, and Africa. As they continue to work toward shared objectives, they will cover more ground together.

Leverage each other's platforms to broaden reach. The proliferation of popular Chinese-designed and -marketed social media apps has the potential to create entirely alternative information ecosystems that China and Russia could jointly leverage. This already occurs in the traditional media space.

Jointly harness technological change. China and Russia are increasingly well positioned to pilot "viral" apps to collect, analyze, and generate data on users in democracies. A major area of focus for their investments in next-generation digital interference capabilities will include controlling the platforms, software, and the manner in which online activities are conducted.

RECOMMENDATIONS

The United States and its democratic allies and partners should adopt a holistic approach to countering digital influence campaigns by China and Russia, particularly in light of the growing synergies between these two powers. The increasing convergence between these actors means there are steps Western democracies can take that will be effective in pushing back against both Russia and China. In practice, this approach should comprise four primary lines of effort.

Bolster Resilience to Digital Influence Campaigns

- *Fund targeted open source research.* To address a critical knowledge gap, the National Science Foundation should ramp up funding for rigorous social science analysis of how online interference by China and Russia shapes the perceptions of citizens in democracies.
- *Expand digital literacy education to adults.* The U.S. Department of Education should partner with a leading information technology company to design a digital citizenship course for American adults, with participation incentivized through small tax rebates.
- *Regulate the social media landscape.* For example, Congress should enact legislation mandating that social media companies label content disseminated by state-sponsored actors.

Expand Coordination among Democracies

- *Red team China-Russia synergies.* This would involve convening officials and technologists from the United States, Europe, Japan, Taiwan, and Australia to explore future digital influence coordination between the world's two leading authoritarian powers.
- *Stress-test existing coordination structures.* The Group of Seven's (G7) Rapid Response Mechanism should conduct an intelligence sharing exercise to identify bottlenecks for disseminating classified information regarding Chinese and Russian influence campaigns.
- *Leverage the Community of Democracies (CoD).* To enable developing countries to combat authoritarian digital interference, the United States should propose a new coordination mechanism within the CoD, which has a more diverse membership than the G7.
- *Act in concert within international organizations.* The United States should work with its democratic allies and partners to advance an agenda in multilateral forums that delegitimizes online influence campaigns by China and Russia and mitigates their potential impact.

Construct and Sustain Healthy Information Ecosystems

- *Support independent diaspora media.* One step could include a partnership between the State Department and a highly credible nongovernmental organization to award grants to Chinese- and Russian-language reporters and media entrepreneurs.
- *Subsidize fact-based content in regions where affordability matters most.* The U.S. International Development Finance Corporation should extend loans and other supports to American media companies looking to grow their presence in developing markets.
- *Catalyze innovative technological solutions.* This could begin with the Defense Advanced Research Projects Agency (DARPA) organizing a "Democratic Integrity Hackathon" to develop products to protect social media platforms against Chinese and Russian digital influence campaigns.[2]

Enhance Efforts to Deter China and Russia

- *Develop a menu for cost imposition.* The United States and its democratic allies and partners should develop a robust set of options to impose costs on China and Russia, with the aim of deterring the most egregious forms of digital influence campaigns. These options should range from demonstrating the ability to hold at risk the personal data of authoritarian elites to injecting fact-based information that exposes regime corruption into the online ecosystems of China or Russia.
- *Establish a declaratory policy.* The United States should quietly convey to China and Russia that it is willing and able to impose costs, particularly with respect to online interference that touches on election integrity.

Introduction

The 2016 U.S. presidential election and the 2018 and 2020 Taiwanese local and presidential elections crystallized Russia's and China's use of digital interference to shift the playing field in the contest between democracies and autocracies.[3] While foreign information operations are time-tested methods of authoritarian influence, the world's hyperconnectivity has opened up new avenues by which information operations can be waged. The proliferation of technology has augmented the capacity of autocrats to shape perceptions about the attractiveness of their governance model, sow chaos in democracies, and downplay antagonism toward their regimes.

Russia's and China's use of digital influence campaigns does not occur in a vacuum. Since 2005, authoritarianism has been on the rise globally.[4] Much of this authoritarian resurgence has stemmed from growing challenges that democracies face inside their own borders, including high levels of inequality, polarization, and citizen dissatisfaction with their governments. These dynamics provide fertile ground for Russia's and China's digital interference campaigns to flourish. Likewise, shifting power dynamics in the international environment have emboldened authoritarian regimes—especially Russia and China—to become more assertive on the global stage. As democracies have become distracted by their own internal problems and Russia and China sense the opportunity to accelerate a shift away from a U.S.-led order, they have increased their use of digital influence campaigns to advance this objective.

Russia and China are learning from each other and deepening their coordination.

Both Russia's and China's digital influence campaigns pose challenges to democracies. But even above and beyond the individual challenges that Moscow's and Beijing's actions pose, the two actors' approaches are converging, making the overall challenge greater than the sum of their individual parts. United by their shared goal to undermine liberal democratic norms and reduce U.S. global influence, Russia and China are learning from each other and deepening their coordination on joint efforts to achieve these goals.

There are myriad challenges that Russian and Chinese digital influence campaigns create, and prioritizing the problem remains difficult for policymakers in democracies. It is still difficult to determine what policymakers should respond to, and what part of these campaigns is simply "noise"—distracting and unwelcome efforts that do not actually change citizen attitudes or concrete policy outcomes in the countries they occur. There are, however, three key areas where Russian and Chinese digital influence campaigns are especially problematic for the health of democracies. First, Russia and China—albeit less systematically, and with a focus on Taiwan—are amplifying polarization and creating divisions in democratic societies in ways that are problematic for democratic governance. Russia in particular is able to weaponize such divisions, creating an unvirtuous cycle of political polarization and digital interference. Disinformation and inflammatory messaging inserted into a polarized society spurs polarization, and as societies become increasingly polarized, disinformation becomes more effective.[5] Polarization is particularly dangerous because it paralyzes democracies and hinders democratic consensus, which undermines faith in the democratic system.

Second, digital influence campaigns targeting elections threaten the health of democracy. As authoritarian-backed actors aim to disrupt democratic elections, foreign election interference foments lasting damage to democracies because it erodes faith in elections and institutions and further polarizes politics.[6] Political trust is already at historically low levels globally.[7] The decay of political trust is supercharged by digital interference efforts by authoritarian actors who aim to make democracy appear dysfunctional and to cast doubt on the efficacy of government institutions and electoral processes. In 2016, Russia's interference in the U.S. presidential election was designed in large part to undermine public faith in the U.S. democratic process.[8] China's digital interference campaigns in the 2018 and 2020 Taiwanese local and presidential elections advanced pro-Chinese Communist Party (CCP) narratives and attempted to shape the information space to counter antipathy toward the regime in Beijing. While Russia and China vary in the breadth of their efforts to disrupt elections, both actors seek to impair democracy's functioning and instill doubt in democracy as a system of governance where such tactics advance their geopolitical interests.

Lastly, the information landscape can create the context for pro-Russia and pro-China narratives to thrive. Over the past decade, media freedom has declined worldwide.[9] The deterioration of independent journalism and local media has created an absence of trusted actors to inform citizens, hold governments accountable, and shine light on foreign efforts to weaken democracies. Without access to accurate and trusted

information, citizens rely on alternate sources for news, including news shared by their online networks or outlets captured by Russia or China—neither of which are held accountable for sharing false news. The propagation of disinformation further erodes conceptions of truth, which makes it harder to distinguish false news from accurate reporting. Russian and Chinese tactics are also designed to weaken the values "glue" that supports Western cohesion and alliances.

Russia's and China's digital influence campaigns require democracies to collectively generate creative solutions to combat the nefarious aspects of digital influence campaigns without posing a risk to freedom and civil liberties at home. This report will explain China's and Russia's goals, the tactics and tools they use to achieve those goals, how their approaches are different, and how they are increasingly converging. It will close with actionable recommendations for democracies to jointly reclaim the narrative and build resilience to inoculate themselves against digital influence campaigns.

Russia's and China's digital influence campaigns require democracies to collectively generate creative solutions to combat the nefarious aspects of digital influence campaigns without posing a risk to freedom and civil liberties at home.

The report's findings and recommendations are informed by a number of inputs. First, the report builds on a comprehensive literature review examining the aims and tactics of China's and Russia's digital influence efforts. The Center for a New American Security (CNAS) also held a series of roundtable discussions examining growing ties between Russia and China, including two sessions focused on Russian and Chinese digital influence. More broadly, the authors have engaged in research and conducted interviews with experts and U.S. and foreign government officials under the umbrella of a CNAS-wide initiative on Countering High-Tech Illiberalism.

The Role of Digital Influence in the Foreign Policy Toolkits of China and Russia

China and Russia view their ability to shape the information environment as critical to advancing their interests and have invested in their capacity to do so globally. For Russia, information warfare is a central pillar of the Kremlin's more assertive foreign policy. While propaganda has long been part of the Kremlin's arsenal—playing a prominent role throughout the Cold War—Russia's conflict with Georgia in 2008 marked an important turning point in the Kremlin's use of information warfare. The Kremlin perceived that Russia lost the battle over the narrative of events in Georgia, underscoring for Moscow the importance of being able to advance Russia's worldview.

The Russian leadership today views the information domain as one of the fundamental arenas in which states compete.[10] Moreover, Russian leaders do not view their hybrid tactics, including information warfare, as being separate from conventional military capabilities. Instead, Russia uses information warfare across the full spectrum of conflict and competition between states, including during peacetime. Russia's digital influence operations—part of its information warfare arsenal—seek to shape the attitudes and policy preferences of an adversary's political, military, and civilian populations. Russia uses digital tools to exert influence and change the political dynamics within countries whose policies are contrary to Russian interests.

Russian information operations have evolved from the time of the Cold War to capitalize on the contemporary information environment. Russian digital influence activities have proliferated across various ministries and agencies of the government as well as private actors. Some analysts have described the weblike structure of Russian operations, encompassing its intelligence community, Ministry of Defense, Ministry of Foreign Affairs, and proxies such as the Russian Internet Research Agency (IRA), which serves as a primary purveyor of curated content and false information on social media platforms.[11] And while the Russian Presidential Administration (PA) broadly dictates the direction of Russian campaigns based on its priorities and agenda, individual actors within this web have considerable latitude to implement the campaigns as they see fit. In other words, President Vladimir Putin and the PA set the overall direction of Russian digital influence activities, but Russian-backed actors often compete to advance these broad directives and have the latitude to act opportunistically and to adapt to local conditions as needed.[12]

A September 2018 paid insert from state-run China Daily *in* The Des Moines Register *attacks the Trump administration's trade policies and calls out their impact on farmers. The Chinese Communist Party has long viewed control over ideas as a core tenet of China's national power and has increasingly sought to apply these concepts of control beyond its borders. (Jennifer Jacobs/Twitter)*

Beijing, too, has long viewed control over ideas as a core tenet of China's national power. The Chinese Communist Party has increasingly sought to apply these concepts of control beyond its borders, and its efforts to shape the global online information environment have gained prominence in the CCP's foreign policy agenda in the last decade. Dating back to the late 2000s at the height of Hu Jintao's leadership, the CCP's Central Propaganda Department (CPD) sharpened its focus on the global "competition for news and public opinion" and "the contest over discourse power" through the "innovation of news propaganda."[13] Shortly after becoming the general secretary of the CCP, Xi Jinping reiterated at the August 2013 National Meeting on Propaganda and Ideology that China needed to "strengthen media coverage … use innovative outreach methods … tell a good Chinese story, and promote China's views internationally."[14] A 2013 meeting of the CPD[15] reiterated that shaping online public opinion was an area of "highest priority" for the party.[16]

Through propaganda, censorship, and strategically motivated economic coercion, Beijing has sought to tighten its chokehold on self-proclaimed "core interests" such as Taiwan; forestall international criticism of its policies toward Hong Kong, Tibet, and Xinjiang; and promulgate narratives about its global leadership.[17] A wide range of state actors have a hand in these efforts, including the Ministry of Foreign Affairs, State Council Information Office, the Central Foreign Affairs Office, the United Front Work Department, the Ministry of State Security, the Ministry of Public Security, and the Cyberspace Administration of China, to name a few.[18] Additionally, on the military side, the reorganization of the People's Liberation Army (PLA) in 2015 and the consolidation of its cyber capabilities into a single service generated significant momentum for Beijing's concept of "information warfare," including through the development and deployment of new platforms.[19]

Mutual Interests Driving Chinese and Russian Digital Influence Operations

Although there is little evidence to suggest that Moscow and Beijing explicitly coordinate their information operations, the two countries are increasingly finding common cause as their interests align on a number of issues and in strategic regions. Given this growing convergence in interests, their digital influence campaigns—although often executed in different ways—work in tandem and toward the same objectives. Chinese and Russian digital influence campaigns, in other words, are largely driven by several complementary geopolitical objectives.

Objective 1: Undermine Liberal Democratic Norms and Institutions

First, China and Russia certainly both use digital influence campaigns in an effort to undermine liberal democratic norms and institutions. China and Russia see liberal democracy as a threat to their own domestic standing and survival. They view U.S. efforts to support democracy as a thinly veiled attempt to expand U.S. influence and undermine their regimes. They believe, for example, that the United States uses democracy to obscure Washington's efforts to foment color revolutions intended to unseat regimes that it views as unfriendly, including in Moscow and Beijing. In August 2019, as the pro-democracy protests in Hong Kong gained momentum, the Russian Foreign Ministry's primary spokesperson, Maria Zakharova, recounted Chinese allegations that the United States had incited the protests and expressed the need for China and Russia to step up efforts to jointly investigate the United States' use of technology to destabilize their two countries.[20]

> **China and Russia see liberal democracy as a threat to their own domestic standing and survival.**

Although China and Russia have long sought to counter Western democracy promotion, China and especially Russia have gone on the offensive since 2014 and are taking the fight to Western democracies. Both countries calculate that weakening democracy can accelerate the decline of Western influence and advance their geopolitical goals.[21] They therefore share an interest in pushing narratives that portray democracy as messy and ineffective, especially relative to their centralized and strongman systems of rule.

Objective 2: Weaken Cohesion among Democratic Allies and Partners

Chinese and Russian digital influence campaigns are also driven by a shared desire to weaken cohesion among democratic allies and partners. Most importantly, China and Russia seek to peel U.S. allies and partners away from Washington to dilute opposition to their interests. China, for example, understood long ago that its rising economic influence would lead other countries to balance against it—an understanding encapsulated in the late paramount leader Deng Xiaoping's foreign policy dictum of "hide your strength, bide your time."[22] Beijing, therefore, uses information operations to portray China's rise as peaceful—particularly as it casts itself as a highly nimble and capable partner in contrast to the United States' retrenchment from global leadership in the throes of the COVID-19 pandemic—and to keep countries from banding with the United States in opposition to it. In Europe, for example, China pursues a divide and conquer approach, calculating that a fractured Europe enhances Beijing's leverage on trade and prevents Europe from taking united actions that violate China's self-proclaimed core interests, such as criticizing the human rights crackdown in Xinxiang, expressing support for democratic Taiwan, and pushing back against Beijing's adventurism and expansionist maritime claims in the South China Sea. Russia similarly seeks to sow division within the European Union (EU) to create conditions conducive to Moscow.[23] Russia sees a divided EU as less capable of pushing back on Moscow and potentially leading to a break in the consensus required to maintain the EU's sanctions on Russia—a key Kremlin objective.[24]

Objective 3: Undermine U.S. Global Influence

Ultimately, Beijing's and Moscow's digital influence operations are driven by a shared desire to undermine U.S. global influence. Beijing and Moscow define their power in terms that are relative to the United States, and they view their efforts to undercut the United States as a means of enhancing their own relative standing in the world. China and Russia seek to use digital influence campaigns to weaken U.S. power—especially American soft power—and Washington's ability to project it in ways that are inimical to their interests. Chinese and Russian diplomats have in official statements, for example, been open about their efforts to pool their countries' know-how and technological and media resources to diminish the United States' global influence.[25]

Objective 4: Advance Chinese and Russian Positions

Just as China and Russia seek to undermine U.S. influence, they also leverage online platforms to build support for their positions. China and Russia endeavor to shape the information environment, discredit critics, and cultivate influence through proxies.[26] These efforts are intended to build support for Chinese and Russian views in countries across the globe. China far more so than Russia seeks to build positive and proactive narratives. The primary aim of China's informational strategy is to "tell a good Chinese story, express China's voice, and get overseas audience recognition and support for Xi Jinping thought."[27] Through propaganda and broader efforts to shape the global information environment, Beijing has peddled narratives about its inevitable ascent to global leadership, touting its advancement of "high-quality" infrastructure development under the banner of Xi's signature Belt and Road strategy while casting its authoritarian rule as more suited to managing crises nimbly and capably than democratic systems.[28]

Although Russian information operations tend to be more destructive than constructive, the Kremlin also seeks to advance pro-Russian narratives. In Europe, for example, Russian information operations seek to build support for conservative social values, while in the Middle East, Moscow is advancing a narrative of the United States as an unreliable and unpredictable partner. In the wake of the United States' withdrawal of troops from northeastern Syria, for example, Moscow sought to portray the United States as a mercurial power, while emphasizing Russia as a responsible peacemaker.[29] Through a steady drumbeat of repetitive messages propagated through multiple channels, Russia uses digital influence campaigns to advance pro-Russian narratives and popularize the Kremlin's version of events.[30]

Through propaganda and broader efforts to shape the global information environment, Beijing has peddled narratives about its inevitable ascent to global leadership.

Different but Converging Approaches to Digital Interference

Over the last several years, Beijing and Moscow have taken different approaches to advancing the shared foreign policy objectives previously discussed. Their respective foreign policy approaches are reflected in the different ways they have executed their digital influence campaigns. Although the differences in their approaches to digital influence are likely to persist, there is growing evidence that the two countries are learning from each other and enhancing their coordination, leading to greater convergence in their digital influence efforts. As we discuss at greater length next, their coordination and convergence suggest that democracies worldwide are likely to see growing synergy between the two authoritarian powers in the information environment. This, in turn, generates unique challenges for democracies globally and for the United States in particular.

Confrontational Versus Under-the-Radar

In general, Russia has been more confrontational and brazen in its approach to digital influence than China, although these lines are being blurred amid more recent geopolitical developments such as the COVID-19 global pandemic. Putin is keenly aware that Russian power will decline. By going on the offensive, including through efforts to manipulate the information environment, the Kremlin seeks to influence the rules of the game while it still has the ability to do so. This urgency and the Kremlin's desire to rewrite the rules of the game mean that Moscow is more risk acceptant in its digital influence operations.

Beijing, in contrast, has pursued a more incremental and diffuse strategy, not unlike the gradually unfolding approach it has deployed in areas such as the South China Sea. The CCP is operating on a longer time horizon than the Putin regime, as Beijing perceives its power and influence to be on an upward trajectory. It is, therefore, spreading the tendrils of its influence slowly and systematically, marshaling multiple vectors of influence as part of a whole-of-society effort, ranging from popularizing Chinese-designed viral apps to co-opting bodies governing cyberspace in international organizations.

Destructive Versus Constructive

Relatedly, China's digital influence operations are more constructive than Russian operations, which are most often destructive and disruptive. For Moscow, the goal is often to discredit the United States and other Western democracies. Russian state and non-state actors seek

to spread disinformation, sow confusion, and exploit divisions to polarize public debates, including through its amplification of hyperpartisan social media accounts.[31] For example, Russian trolls working for the Internet Research Agency continue to seek to amplify racial divisions in the United States ahead of the 2020 elections, in large part to inflame divisions among Americans and provoke social unrest.[32] In these ways, the Kremlin seeks to make it hard for citizens to arrive at a shared understanding of events and ultimately to amplify distrust in governments and institutions.

For Beijing, in contrast, the CCP seeks to create positive perceptions of China and to legitimate its form of government.[33] In particular, the CCP seeks to advance the appeal of Chinese culture, values, and traditions. For example, through commentators hired by state authorities, unofficially known as the "50 Cent Army" because of early allegations that employees would be paid 0.50 yuan per online post, the CCP has sought to craft, disseminate, and amplify pro-Beijing narratives online to shape perceptions around its policies.[34] A preference for promulgating a stable narrative that enables Beijing to build economic ties, export its telecommunications infrastructure, and build long-term influence runs as a common thread across these activities—as reflected in frequently repeated slogans such as "win-win cooperation" and "community of shared future for mankind."[35] Where China has shown capacity to push negative narratives and undermine trust in democratic institutions, as in the cases of Taiwan and Hong Kong, it has relied on creating spam accounts or leveraging extant accounts on unrelated topics to dilute and weaken the overall information space.[36]

Flooding Versus Suppression[37]

Finally, China's approach to shaping the information environment is different from Russia's in that China also often seeks to censor or deny access to information, while Russia primarily seeks to flood social media with coordinated, inauthentic tactics.[38] China is able to use its economic leverage and market potential to muzzle even American companies and suppress online information that is unfavorable to CCP interests. Apple Inc., for example, buckled under pressure from the Chinese government and removed from its online store the app HKmap.live, which helped Hong Kong protesters in 2019 track police movements, after a Chinese state-owned newspaper criticized the U.S. technology giant for allowing the software on its platform.[39] During the same period, Apple also removed the Taiwanese flag emoji from iPhones in Hong Kong and Macau.[40] Apple's acquiescence is only one example of broader trend lines of American corporations modifying their online presence to appease Beijing and the market that it represents.

Beyond its coercion of corporate America, Beijing has exploited the lack of reciprocity between the information ecosystems of China and democracies to advance its agenda. While American social media platforms—including Facebook, Instagram, YouTube, Twitter, WhatsApp—are increasingly difficult to access within China's borders, especially since the CCP's crackdown on virtual private networks (VPNs) in the lead-up to its 2017 Party Congress, China's own tech champions promulgate their alternative platforms beyond Chinese borders.[41] These platforms provide Beijing with the capacity for widespread censorship, often without users' awareness. Preliminary analysis, for example, suggests that content on TikTok—one of the world's fastest-growing social media platforms and the most downloaded app worldwide in the first quarter of 2019—may be subject to China's censorship apparatus by way of its Beijing-based parent company, ByteDance.[42] And the censorship concerns around WeChat are already well documented.[43] During the protracted pro-democracy struggle in Hong Kong in 2019, the CCP's censorship machinery hummed along at full throttle as Tencent suspended the accounts of WeChat users, even in the United States, who criticized Beijing.[44]

People hold up smartphone lights and posters during a "mums protest" against alleged police brutality and the proposed extradition treaty in June 2019 in Hong Kong. Apple succumbed to pressure from the Chinese government and removed from its online store the app HKmap.live, which helped Hong Kong protesters to track police movements. (Carl Court/Getty Images)

Moscow diverges from Beijing in its capacity for censorship. Rather than suppressing information, Russia uses a tactic that some scholars have referred to as "flooding," or the dissemination of high volumes of repetitive information across a large number of channels.[45] In other words, Russian-backed actors seek to seed "public debate with nonsense, disinformation, distractions, vexatious opinions and counter-arguments."[46] In this way the Kremlin does not seek to dominate the informational space, but dilute it.[47] For example, when faced with a damaging event like the Skripal poisoning, the Russian government's response (operating in part through state-controlled media) was to flood the informational space with potential explanations, however implausible.[48]

Chinese and Russian Digital Influence Campaigns are Converging

Despite these important differences in their approaches, China appears to be gleaning best practices from Moscow and has begun to adopt some of the Kremlin's tactics. As China adopts these tools, Beijing also appears to be gaining confidence with these approaches and has become more willing to accept risk with its digital influence efforts. In short, there is growing convergence in the digital efforts of China and Russia, with Beijing growing more aggressive in its actions.

The growing similarity between China and Russia has been most apparent in the social media domain. As one former political science lecturer at Tsinghua University observed, "China has been studying the propaganda strategies of Russia, including how the latter manipulates media, mobilizes its youth and trains its hackers."[49] In a July 2019 Study Times article, for example, Hua Chunying, director of the Ministry of Foreign Affairs (MOFA) Information Department, outlined a more aggressive global social media strategy that suggested Twitter would become an important tool in Beijing's information warfare arsenal.[50] During a November 2019 conference that the United Front Work Department organized on conducting internet influence activities, the department's head noted that the United Front would enable social media influencers and other prominent social figures to "play an active role in guiding public opinion."[51] Shortly thereafter, in December 2019, China's MOFA opened an official Twitter account, which posts regularly on topics ranging from its self-proclaimed global leadership amid the coronavirus (COVID-19) crisis that originated in Hubei province in 2019 to its advancement of "high-quality" development through the Belt and Road to scathing criticism of the United States' unilateralism.[52]

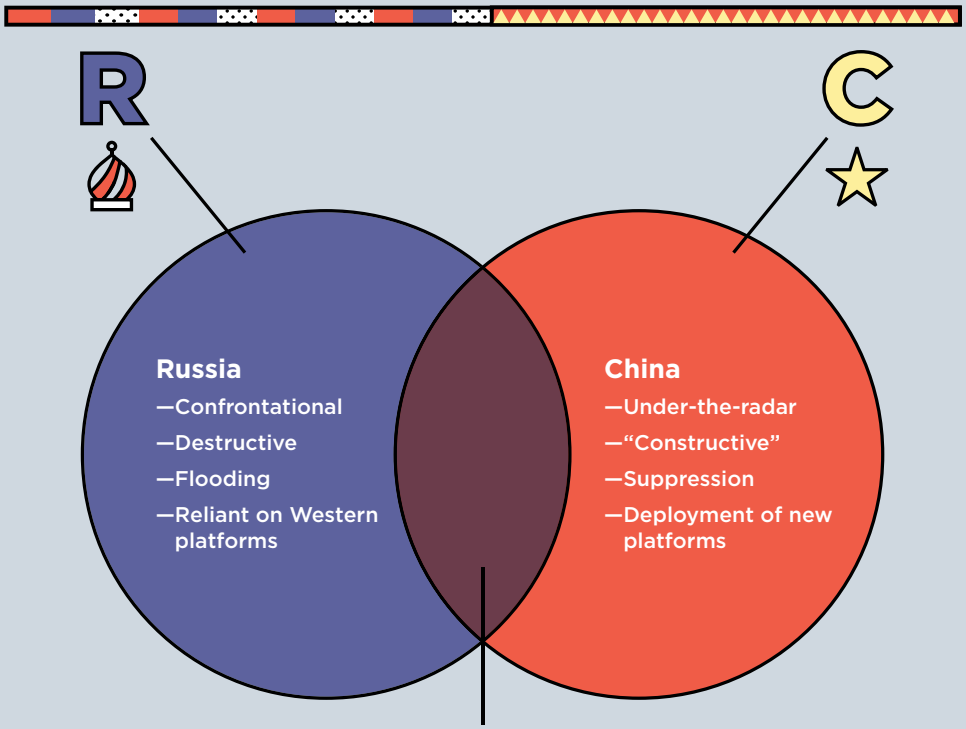
CHINA'S FORAY INTO ELECTION INTERFERENCE

In the lead-up to Taiwan's local elections in November 2018, Beijing unleashed a full-throated assault on Taiwan's online information space, bombarding citizens with content detrimental to President Tsai Ing-wen and the Democratic Progressive Party (DPP)—which seeks greater autonomy from China.[53] The People's Liberation Army leveraged social media accounts on Facebook, Twitter, Line, Weibo, and other online platforms to pollinate these narratives, which were in turn amplified by China's "50 Cent Army" of government-paid commentators and bots. Meanwhile, Taiwanese news outlets unwittingly incorporated photographs and video content from these falsified accounts into their reporting.[54] The government of Taiwan moved quickly to plug holes and recalibrate the information space prior to the 2020 presidential election, including through the passage of its Anti-Infiltration Act to address loopholes in campaign funding and foreign influence campaigns that leverage civil society. Nonetheless, Beijing may be closely observing Russian interference tactics in the United States' presidential election in 2020 and viewing it as an opportunity for learning—or in the least, a moment of potential democratic dysfunction to exploit.[55]

Beijing may be closely observing Russian interference tactics in the United States' presidential election in 2020 and viewing it as an opportunity for learning.

But even as Beijing is increasingly positioning itself to leverage Facebook and to conduct strategic messaging beyond its borders, its tactics on these American platforms have thus far largely remained rudimentary.[56] At the height of Hong Kong's pro-democracy protests in 2019, for example, Beijing applied blunt force tactics to try to warp the narrative around its policies, appropriating hundreds of thousands of accounts to seek to discredit the protesters, including by labeling them as agents of the United States.[57] After Twitter removed nearly a thousand accounts and suspended 200,000 others that originated from China, Beijing rebutted the United States' criticism of its practices with the accusation that American platforms were in fact censoring legitimate views held by Chinese citizens.[58]

China appears to be gleaning best practices from Moscow and has begun to adopt some of the Kremlin's tactics.



Although key differences in Chinese and Russian approaches are likely to persist, there is growing evidence that the two countries are learning from each other and enhancing their coordination, leading to a growing convergence in their digital influence efforts.

Digital Influence Tools Used by China and Russia

Beijing and Moscow retain a largely distinct set of approaches to exercising their influence online, but even so, there are important areas of overlap in the tools they deploy. Even where these convergences are due to happenstance rather than explicit coordination, the areas of similarity and difference in their approaches merit closer scrutiny.

Direct Advertising

Direct advertising is an important vector of disinformation. First, it incentivizes websites to prioritize page views to increase advertising revenue, which contributes to the spread of sensationalized information. Second, advertisements can be microtargeted to extremely specific demographics based on user data, which helps propagators of disinformation reach their intended audience much more effectively.[59]

CHINA

Beijing uses advertisements to promote content produced by its state-sponsored media outlets and companies that support those narratives. Chinese media companies do not have strong reputations as impartial sources outside of China, so their content is unlikely to be effective on its own merits.[60] Therefore, they rely on extensive advertising to spread the message to as many consumers as possible. Despite the fact that the social media platform is banned inside China, Facebook receives approximately $5 billion in Chinese ad buys annually, though only a fraction of that comes from state-sponsored media.[61] It also comes from companies like Huawei, whose ads on social and digital news media urge the public not to trust warnings about them issued by the U.S. government.[62] Beijing recognizes the coercive utility of its large ad buys even in countries with freedom of the press. Locally based Chinese-diaspora media outlets, which often play an important role in diaspora communities, are typically not resilient to threats made by mainland or pro-Beijing advertisers to pull ad revenue unless the outlet refrains from reporting on matters that would anger Beijing."[63]

RUSSIA

Direct advertising is a force multiplier for Russia's extensive digital influence campaigns over social media. Moscow used thousands of advertisements to boost the audience consuming content created by infamous disinformation mills such as the Internet Research Agency to millions of American internet users during the 2016 election.[64] Organizations including the IRA used direct advertising to spread microtargeted messages to a diverse array of demographic and political groups, often simultaneously to both sides of a particular argument in order to sow chaos and exacerbate societal tensions.[65] In contrast, during the 2017 German elections, Moscow targeted Germany's Aussiedler (ethnically German repatriates from former Soviet republics) community with Russian-language advertisements to bolster the group's support of the right-wing populist Alternative for Germany (AfD) party.[66] The community's trust of Russian sources positioned Moscow to subtly influence their opinions through disinformation campaigns.[67]

SIMILARITIES

- China and Russia both create disinformation and then use advertising strategies to augment its spread and influence abroad.
- China and Russia have used advertising strategies to influence the narrative inside diaspora communities located in countries with strong commitments to digital freedom.

DIFFERENCES

- Beijing does not use microtargeting in the same way Moscow does. China's focus is most often broad, using advertisements to spread disinformation to as wide a group as possible until the story sticks, whereas Russia's strategy often involves inciting specific segments of society with highly targeted advertisements.
- The content boosted through Chinese digital ad campaigns is almost always directly related to an issue in which China is involved, whereas with Russian campaigns, the ties to Moscow are often more obscure.

Astroturfing and Co-option of Credible Voices

Though astroturfing can take many forms, in essence it is the practice of obscuring the origin of an idea or message that would appear less credible if the audience knew its true origin. An entity such as a government or political organization could disguise an influence campaign by making it appear as though it were organically originating from local politicians, civil society organizations, or civilians, when the support is actually manufactured.

CHINA

Beijing has used government-organized nongovernmental organizations (GONGOs) to infiltrate places created for civil society and promote the CCP's agenda through influencing norms. Chinese GONGOs and private-sector enterprises act as proxies to advance the goals of the CCP at the United Nations through injecting Beijing's norms into regulatory discussions. China has 25 member organizations in the standardization and development sectors of the International Telecommunication Union (ITU), the U.N. agency responsible for international coordination of information technology.[68] These member organizations include companies that are on the forefront of stimulating the international proliferation of Beijing's invasive cyber norms, such as Huawei, Hikvision, and ZTE.[69] Beijing has also leveraged the reputation of Taiwanese media outlets to publish pieces written by CCP front organizations in order to artificially inflate the perception of pro-mainland sentiments in Taiwanese society.[70]

RUSSIA

Moscow's astroturfing through the use of social media troll farms and bots during the 2016 presidential election is well documented.[71] Russia is attempting to repeat the effort in the 2020 election using the same technique of amplifying socially divisive issues, though the approach may be more elaborate this time.[72] Moscow recently created a GONGO in Ghana that turned several Ghanaians and Nigerians into unwitting proxies.[73] Astroturfing through people and organizations not consciously or overtly connected with Russia makes these endeavors even more difficult to track.[74] Russia has also put effort into astroturfing European news organizations. For example, many media markets in countries such as Serbia and Moldova get their news almost entirely from the same few Russian sources, such as Sputnik, and sometimes even rebroadcast them as local reporting.[75]

Also part of Russia's toolkit is its ability to create and leverage a network of local, pro-Russian voices to

THE RISE OF CHINESE "GONGOS"

One tactic employed by China to marginalize its critics within international organizations and promote favorable voices is the creation of government-organized nongovernmental organizations, or GONGOs. This is a type of international astroturfing. A nonexhaustive list of China's GONGOs includes the following:

Internet and Media

- China Writer's Association
- All-China Journalists Association
- Internet Society of China

Labor and Migrants

- Beijing Yilian Labor Law Aid and Research Center
- Suzhou Migrant Workers Home
- Shenzhen Chunfeng Labor Disputes Services Center

Law and Governance

- Justice for All
- Equity & Justice Initiative
- Dongjen Center for Human Rights Education and Action

Environment

- Huai River Eco-Environment Research Center
- Center for Legal Assistance to Pollution Victims
- Center for Environment Development and Poverty Alleviation

Ethnic Minorities

- Preservation and Development of Tibetan Culture
- Yothok Yonden Gonpo Medical Association
- Lanzhou Chongde Women Children Education Center

Education

- Guangzhou Grassroots Education Support Association
- China Zigen Rural Education & Development Association
- Beijing Hongdandan Education and Culture Exchange Center

Source:
Organizations retrieved from China Development Brief's NGO Directory, http://www.chinadevelopmentbrief.cn/directory/.

advance Russian narratives. Russian networks include academics, news anchors, local politicians, and non-profit organizations. The Kremlin uses these networks to advance Russia's worldview and distract from events that could be unfavorable to Russia.

SIMILARITIES

- Both China and Russia use GONGOs in their digital influence campaigns, though China uses them much more extensively to bend international norms and rules in order to make environments more permissive to its tactics.
- Both China and Russia extensively astroturf social media platforms with bot accounts and paid trolls. Still, whereas China focuses most of its efforts internally on its own networks, on which it fabricates almost half a billion inauthentic pro-government comments a year, Russia is much more outwardly focused with its bots and trolls.[76]

DIFFERENCES

- Beijing astroturfs to censor and co-opt narratives to promote a positive image of China. When their government ties are unknown, GONGOs also improve China's image abroad because they telegraph multilateral engagement and a robust civil society.
- Russia astroturfs to dilute the information environment so that truth becomes unrecognizable, as Moscow favors instability in civil society and democratic institutions.

Propagating Influence Tools

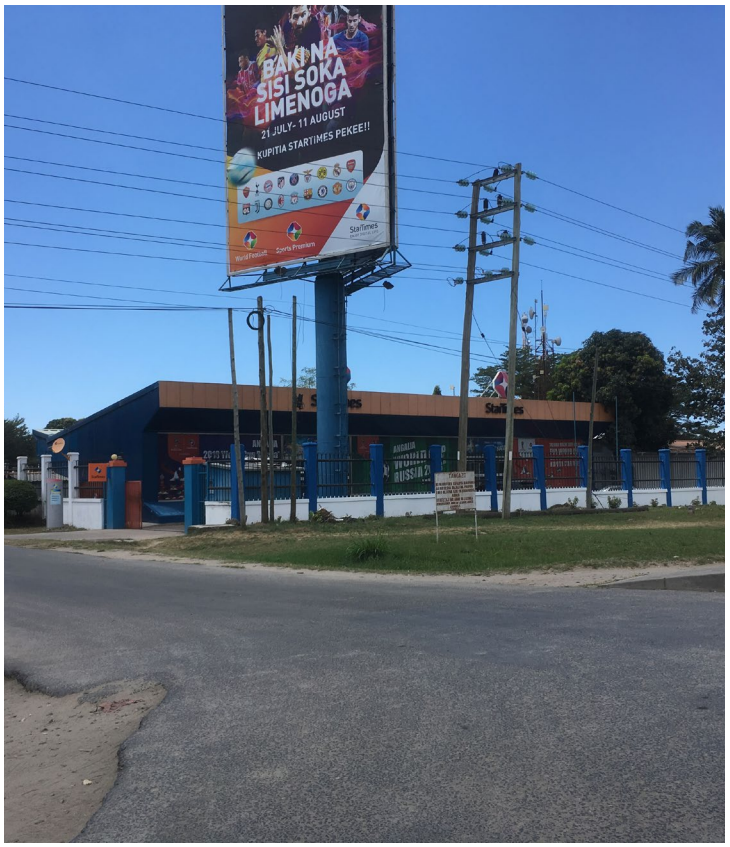
Governments worldwide increasingly have access to models, tools, and expertise conducive to conducting their own digital influence campaigns domestically. This further pollutes the online space and renders China's and Russia's own efforts more effective.

CHINA

China's drive to bankroll and build infrastructure enabling online surveillance and censorship through its Digital Silk Road has facilitated the widespread adoption of systems that mirror Beijing's own.[77] This has affected information environments across the globe, particularly in regions such as Southeast Asia where the challenges to online freedom have never been stronger than in recent years.[78] Outside the Indo-Pacific, Tanzania and Uganda have passed restrictive laws on online media based on China's models of censorship that sacrifice individual freedoms in order to support broader social stability.[79] Beijing also leverages civil society to shape the online space in other countries. The Chinese GONGO China Federation of Internet Societies, whose stated goal is to strengthen the CCP's influence over the internet industry, has held Chinese partnership symposia in Kenya, Tanzania, Cuba, and Brazil.[80] As far back as 2010, Beijing provided equipment and training that enabled Ethiopia's ruling party to surveil internet activity for content critical of its regime and jam uncensored TV and radio signals from Western stations such as Voice of America and DW News.[81]

RUSSIA

Russia has provided ready-made digital strategies to authoritarian leaders. A Russian company with close ties to the Kremlin equipped former Sudanese President Omar al-Bashir with a comprehensive plan that included use of social media to discredit the unrest that eventually led to his ouster in 2019.[82] Burmese soldiers who had



A billboard and storefront in Tanzania advertising StarTimes, a Chinese television provider with a strong presence in Africa. Tanzania has enacted legislation restricting online freedom that is modeled on Beijing's own domestic controls. (StarTimes by Ali A. Fazal/CC BY-SA 4.0)

China's drive to bankroll and build infrastructure enabling online surveillance and censorship through its Digital Silk Road has facilitated the widespread adoption of systems that mirror Beijing's own.

been trained by their Russian counterparts to use disinformation on social media conducted at least one major social media disinformation campaign at the height of the Rohingya refugee crisis.[83] Russia has also become a source of social media bots, one of its government's most highly used disinformation tools, for actors in other countries. A digital influence campaign during the 2018 election in Malaysia relied on bots that were created in Russia. Though the identities of the operators were never revealed, experts believed that it was a Malaysian who purchased the bots from Russia.[84] Similarly, a disinformation company in Mexico that has run influence campaigns for several politicians often purchases its bots from Russian bot farms.[85]

SIMILARITIES

- Both China and Russia actively attempt to facilitate democratic backsliding when they export the oppressive tools that they have honed domestically.
- Both China and Russia have directly trained and advised foreign government actors to strengthen their control through effective digital influence campaigns.

DIFFERENCES

- China's one-stop-shop approach to diffusion is focused on assisting countries to establish a systematic approach to censorship and information control, as well as the proliferation of the infrastructure necessary to sustain it.
- Russia's approach is to supply the digital influence tools, plans, or training to interested foreign actors, but with little effort invested in assisting with the long-term infrastructure to sustain their use.

Coercion and Censorship of Companies Online

Authoritarian governments, particularly China, are able to leverage their countries' market potential and economic entanglement with democracies to shape the preferences and behavior of companies—including those based in the United States—that operate internationally. This has significant implications for how these firms conduct their online operations.

CHINA

Just as Beijing silences domestic political dissent through blunt force intimidation, it uses its economic heft to pressure foreign corporations to demand that they suppress online information that is damaging to the CCP. In recent years, various Chinese government agencies have bullied companies, including Zara, American Airlines, and Marriott, into removing references to Taiwan as a country on their websites.[86] And after a tweet by the manager of the Houston Rockets in support of pro-democracy protests in Hong Kong, Disney and ESPN provided guidance to employees that curtailed discussion of Chinese politics online and on air.[87] While Beijing's crackdown on VPNs makes American social media platforms even more difficult to access within China's borders,[88] China's own technology champions promulgate their alternative platforms abroad.[89] As they go global, these companies remain responsive to Beijing's domestic system of digital censorship and control.

RUSSIA

Russia's attempts to hide information have typically been limited in scope and caused public outcry. For example, Russia's regulator and censor compelled Facebook to remove a page promoting a 2014 rally for opposition leader Alexei Navalny. However, that blockage generated more attention and new pages promoting the rally, which Facebook subsequently refused to remove. Platforms such as Twitter and YouTube rejected Moscow's directives to remove the content entirely.[90] In 2018, Russia's censor directed Facebook-owned Instagram and Google-owned YouTube to remove corruption accusations made by Navalny. Instagram complied but YouTube did not.[91] Though Russia threatens them with fines and blockages, American social media companies have largely escaped severe penalties and—unlike in China—none have been banned in Russia.[92] However, Moscow has shown a willingness to ban major platforms over noncompliance

with a law requiring data on Russian users to be stored on servers located within Russia. Though LinkedIn was blocked for that in 2016, Facebook and Twitter have only been fined and threatened for refusing to comply.[93]

SIMILARITIES

- China and Russia have used lawfare, including data storage and cybersecurity laws, as a premise for banning—or at least temporarily blocking—American social media companies from operating in their domestic online spaces.
- China and Russia have pressured American social media companies, including Facebook, to remove content that supports activists and political or social movements within their borders.

DIFFERENCES

- Russia has used economic pressure toward less ambitious aims than China and has struggled to unilaterally implement its censorship agenda. Moscow uses censorship to focus primarily on managing the narrative within its borders, while the CCP attempts to leverage censorship to shape its international image more broadly.
- In contrast to Russia's primary area of focus, China's pressure tactics extend far beyond social media companies to the online presence of a constantly widening range of corporate entities, including the entertainment, aviation, and service industries.

COMPARISON OF CHINA'S AND RUSSIA'S APPROACHES TO SHARED DIGITAL INFLUENCE TOOLS

Tools	Similarities	Differences
Direct Advertising	▪ Using advertising strategies to augment the spread and influence of their disinformation campaigns abroad. ▪ Using advertising strategies to influence the narrative inside diaspora communities located in countries with strong commitments to digital freedom.	▪ China uses ads to spread disinformation to as wide a group as possible until the story sticks, whereas Russia's advertising strategy often targets highly specific segments of society. ▪ Content boosted through Chinese digital ad campaigns is almost always directly related to an issue in which China is involved, whereas with Russian campaigns, the ties to Moscow are often more obscure.
Astroturfing	▪ Astroturfing through GONGOs, though China uses them much more extensively to bend international norms and rules in order to make environments more acquiescent to its tactics. ▪ Extensively astroturfing social media platforms with bot accounts and paid trolls. China's focus is much more internal than Russia's, which is much more externally focused.	▪ Beijing astroturfs to censor and coopt narratives to promote an image of a responsible and internationally engaged China. ▪ Russia astroturfs to dilute the information environment so that truth becomes unrecognizable, as Moscow favors instability in civil society and democratic institutions.
Diffusion of Interference Infrastructure and Techniques	▪ Actively facilitating democratic backsliding by exporting the oppressive tools that they have honed domestically. ▪ Directly training and advising foreign government actors to strengthen their control through effective digital influence campaigns.	▪ China's one-stop-shop approach to diffusion focuses on assisting countries establish a systematic approach to censorship and information control, and the infrastructure necessary to sustain it. ▪ Russia's approach is to supply the digital influence tools, plans, or training to interested foreign actors, with little to no effort in terms of assisting with long-term sustainability.
Coercion and Censorship of Companies Online	▪ Using lawfare as a premise for banning or temporarily blocking American social media companies from operating in their domestic online spaces. ▪ Pressuring American social media companies to remove content that supports activists and political or social movements within their borders.	▪ Russia has struggled to unilaterally implement its censorship agenda. Moscow uses censorship of companies to primarily focus on managing the narrative within its borders, while the CCP attempts to leverage censorship to shape its international image more broadly. ▪ China uses its domestic market size as leverage for pressure tactics that extend beyond social media companies to the online presence of an ever-wider range of corporate entities including the entertainment, aviation, and service industries.

How Chinese and Russian Digital Influence Efforts are Mutually Reinforcing

Notwithstanding important differences in the goals, methods, and constellation of actors and institutions involved in Chinese and Russian digital influence activities, their convergent interests—particularly vis-à-vis the United States—are increasingly symbiotic.

Magnifying Impact through Complementary Approaches

Although China's and Russia's approaches are often different and seemingly uncoordinated, taken together, they are having a more corrosive effect on democracy than either would have single-handedly.[94] Russia propagates narratives designed to undermine trust in institutions and elected governments. Its disinformation campaigns seek to create an environment in which citizens are unable to discern what is true. And its repetitive narratives about the inefficacy of Western democracy serve to undercut citizens' confidence in the United States and liberal democracy. This creates fertile ground for Chinese narratives to take root.[95] A loose tactical division of labor is already emerging between Beijing and Moscow's digital influence activities. While Russia weakens information spaces by sowing false narratives and flooding platforms with content intended to smear American institutions, Beijing is able to swoop in with positive alternatives and an arsenal of affirmative messaging about the primacy of Chinese technology and about China's ability to provide global leadership amid U.S. retrenchment.

Amplifying Narratives

Relatedly, while there is currently no evidence that China and Russia are coordinating their messaging, there are a growing number of instances in which Chinese and Russian narratives overlap, amplifying the impact of such messages. For example, there are a number of cases in which Russian outlets have propagated pro-Beijing views on a wide range of topics, ranging from China's repression of ethnic Uighurs in Xinjiang to its protracted trade dispute with the United States. The Kremlin is, in effect, actively amplifying Beijing's desired messaging and helping the CCP to blur the lines between news and state propaganda.[96] Pro-Russian new media, for example, have sought to cast doubt on China's detention of ethnic Uighurs in Xinjiang,[97] while Chinese diplomats, in turn, promote this content on their social media profiles.[98] In doing so, Chinese and Russian media and diplomatic institutions have forged symbiotic relationships that support the creation of an entirely alternative information ecosystem in which truth is called into question.

Legitimizing Norm Change

Russia and China are working together to jointly advance their preferred models of online surveillance, censorship, and broader visions of internet governance in multilateral forums, most notably in the United Nations. By changing norms, Russia and China hope to create an information environment conducive to their objectives. Beijing has quietly proselytized its walled-off version of the internet as a model for other illiberal countries around the world to emulate. In its first-ever white paper on international cyberspace cooperation, jointly published by the Ministry of Foreign Affairs and the Ministry of Public Security in March 2017, the CCP committed to leading the "institutional reform of the UN Internet Governance Forum" to position China to play a larger role in shaping the global future of internet governance.[118] Later in 2017, the Chinese Academy of Cyberspace Studies called for the "establishment of a multinational, democratic and transparent global internet governance system" through the United Nations—alluding to a "multilateral" approach to internet management favored by China, Russia, and other authoritarian countries.[119] And in October 2019, the Cyberspace Administration of China held the sixth iteration of its World Internet Conference in China's Zhejiang Province, featuring public- and private-sector representatives from around the world.[120]

As Beijing jockeys for influence and leadership in international organizations, it has joined hands with Russia at the U.N. to promote standards of surveillance and censorship internationally that would further exacerbate the lack of reciprocity between the information ecosystems of the United States and China. In November 2019, the United Nations adopted a cybercrime resolution jointly backed by China and Russia titled "Countering the use of information and communications technologies for criminal purposes."[121] The resolution stands in stark contrast to the norms that the United States and its allies have championed, including maximal access to the global internet, and instead seeks to equip authoritarian governments with broad-based authority to take down websites critical of governments and punish, repress, and censor political dissent online.[122] Activists in liberal democracies have argued that authoritarian governments could leverage the resolution to criminalize online activities that journalists and other members of civil society rely on, such as encrypted chat applications, for day-to-day work.[123]

THREE SNAPSHOTS OF SYNERGISTIC DIGITAL INFLUENCE CAMPAIGNS

Hong Kong

As both China's and Russia's relations with the United States have deteriorated, news media in both countries began to propagate false information about Washington's role in fomenting various destabilizing political events. In August 2019, as the pro-democracy protests in Hong Kong gained momentum, the Russian Foreign Ministry's primary spokesperson, Maria Zakharova, recounted Chinese allegations that the United States had incited the protests and expressed the need for China and Russia to step up efforts to jointly investigate the United States' use of technology to destabilize their two countries.[99]

Likewise, in December 2019, amid the pro-democracy protests in Hong Kong, RT—an English-language news channel that American authorities have deemed a propaganda arm of the Kremlin—released a documentary called Hong Kong Unmasked, which condemned the Central Intelligence Agency and U.S. nongovernmental organizations such as Freedom House and the National Endowment for Democracy for spurring the protests in Hong Kong.[100] In ensuing weeks, RT's documentary in turn garnered substantial praise on Chinese social media platforms for offering a "true accounting" of the events in Hong Kong. Russia's Federal News Agency, which is part of the Kremlin-backed Internet Research Agency, similarly debased Hong Kong pro-democracy protests by fabricating inflammatory quotes and attributing them to protesters.[101]

Fifth-Generation Wireless Technology (5G)

Beyond seeking to denigrate the United States' international reputation, state media and propaganda apparatuses in China and Russia have also sought to affirmatively shape the political debate around issue areas with outsized geopolitical ramifications, such as 5G deployment. Huawei has, independently, pursued a concerted and highly creative public diplomacy campaign across Europe tapping into conversations about European values. In 2019, Huawei spent more than $3 million on direct advertising and lobbying, outpacing the combined spending of its European 5G competitors, Ericsson and Nokia, and far exceeding its American rival Qualcomm.[102] Huawei's efforts included taking out advertisements in leading publications such as Politico Europe, livestreaming public debates with members of the European Parliament, and mailing press packets to hundreds of journalists.[103]

Notably, as Huawei's equities in Russia have expanded, Moscow has also championed the Chinese tech giant's cause while denigrating the United States' policies toward the company. During Xi Jinping's June 2019 visit to the St. Petersburg International Economic Forum,

RT, an English-language news channel that American authorities have deemed a propaganda arm of the Kremlin, promotes the documentary Hong Kong Unmasked on Twitter. The documentary blamed the Central Intelligence Agency and U.S. nongovernmental organizations such as Freedom House and the National Endowment for Democracy for spurring the protests in Hong Kong, and garnered substantial praise on Chinese social media. (RT/Screengrab)

Vladimir Putin accused Washington of instigating a "technological war of the coming digital era" by blocking Huawei for American networks and urging allies to follow suit.[104] Russia's propaganda apparatus followed suit. While RT aggressively promoted false information about the deleterious health effects of 5G expansion in the United States and Europe,[105] it has touted Huawei's role as a leading corporate innovator, including through a series of flattering "exclusives" at Huawei company headquarters.[106] And just as Huawei signed a deal with Russia's largest cell carrier to roll out the country's first 5G wireless network and to upskill 10,000 Russian technicians on the use of advanced technologies, Russian diplomats and Russian state media began to hail Huawei's standing as a global standard-bearer of innovation.[107]

COVID-19

In some instances, Russian influence activities on social media platforms have echoed, mirrored, and yielded secondary benefits for China. A report by the European Union's External Action Service, for example, noted that between the end of January 2020 and the beginning of March 2020, there had been more than 80 cases of disinformation about COVID-19 linked to pro-Kremlin media.[108] Prominent outlets such as the Russian government-funded RT cast a pall over the United States' response to the pandemic, repeatedly indicating that U.S.

officials were seeking to exploit the outbreak for their own gain and that the U.S. government was politicizing assistance while Russia and China were stepping in to fill the void of global leadership.[109] A U.S. State Department report in early 2020 also indicated that thousands of social media accounts were propagating false information about the COVID-19 outbreak, including a conspiracy theory that the virus was engineered by the United States as an agent of biological warfare against China—and Russian actors were potentially amplifying these narratives. One such conspiracy theory claimed that the U.S. Department of Defense had generated the virus to target China. These types of influence operations were consistent with the efforts of Russian agents to sow discord amid the 2016 presidential election in the United States through coordinated activity amplified by automated bots and trolls.[110]

Chinese social media also picked up the threads of these manufactured narratives and teemed with elaborate conspiracy theories implicating the United States and other democracies for instigating the spread of the virus. In one particularly sophisticated scheme to pin blame on the United States, the Chinese Foreign Ministry's Information Department launched a concerted Twitter campaign to circulate fabricated "scientific" articles by Chinese civil think tanks alleging that COVID-19 had been manufactured in U.S. Army biodefense labs and that American soldiers had unwittingly brought the virus over to China during the Military World Games in October of 2019.[111] The articles featured screenshots of headlines from leading American newspapers, such as *The New York Times,* which—taken entirely out of context—seemed to support Beijing's claims.[112] Some Chinese Communist Party agents on Twitter even contended that American soldiers participating in the military games had deliberately shed the virus at the Huanan Seafood Market, which is largely presumed to be ground zero of the global pandemic.[113] Other reports by Chinese state media sought to muddy the waters by suggesting that the disease had initially appeared in Italy before it emerged in Wuhan, China, at the end of 2019.[114]

All of these false narratives ultimately laid the groundwork for China to play up its global leadership in the response to COVID-19 and for Russia to champion Beijing's efforts. On Twitter, for example, Chinese diplomats sought to favorably portray Beijing's handling of the outbreak through a panoply of formats, including crudely doctored or staged video clips featuring citizens in Italy, Angola, and countries across Asia expressing gratitude to China for their provision of medical expertise, masks, testing kits, and other public goods.[115] How these narratives are received among audiences hard-hit by the pandemic remains an open question, however.

Perhaps no country has felt the brunt of China's online influence operations amid the height of the COVID-19 pandemic more acutely than Italy. In a two-week period in March 2020, for example, nearly 50,000 tweets flooded the Twittersphere with pro-China hashtags.[116] Notably, nearly half of tweets featuring the hashtag "forzaCinaeItalia" (Go China, go Italy) and more than a third of tweets featuring the hashtag "grazieCina" (thank you, China) stemmed from bots—a quintessentially Russian tool that Chinese operations have increasingly leveraged—that averaged more than 50 tweets per day that were unequivocally favorable to China's COVID-19 diplomacy.[117] All of this points to a comprehensive, well-coordinated information operation aimed at bolstering China's standing as a net provider of public goods.

Houlin Zhao of China at the 2018 elections of the International Telecommunication Union in Dubai, where he was reelected as secretary-general. China and Russia jointly seek to advance their authoritarian digital model in international forums. (ITU/D. Woldu)

China and Russia are together advancing alternative multilateral frameworks at the working level within the United Nations as well. This includes seeking to jointly mobilize illiberal actors to control, modify, and dilute resolutions coming out of international organizations and bodies that protect freedom of expression and access to fact-based information. For example, after the U.N. Group of Governmental Experts (UNGGE) published a report affirming the application of international law to state military use of cyberspace, China and Russia launched their own parallel process, the Open-Ended Working Group (OEWG), criticizing the UNGGE for its failure to accommodate the preferences of developing countries.[124] And while Beijing and Moscow have claimed that they are advancing "more democratic, inclusive, and transparent" ways of regulating online activities, they denied some nongovernmental organizations (NGOs) and other civil society groups accreditation for participation in OEWG processes.[125]

By chipping away at norms governing the free flow of information on the highest stage of international cooperation, China and Russia are together seeking to bend the arc of the global information architecture to their advantage.[126] This means that while their own online ecosystems are increasingly segmented from the rest of the world, Beijing and Moscow are able to continue to exploit the relative openness of the United States' and other democracies' information environment to manipulate the narrative around their policies and advance their agendas. Additionally, as China and Russia increasingly seek to shape international norms around surveillance and censorship through coordinated action in the U.N. and other international bodies, they are making it easier for countries with weak democratic or authoritarian-leaning institutions to silence online dissent by deeming it "criminal activity." In effect, the two countries are working together to mobilize and lead coalitions of illiberal states to undercut online civil liberties and the right to freely access accurate information globally and more broadly to render ineffectual institutions that are designed to protect human rights.

By chipping away at norms governing the free flow of information on the highest stage of international cooperation, China and Russia are together seeking to bend the arc of the global information architecture to their advantage.

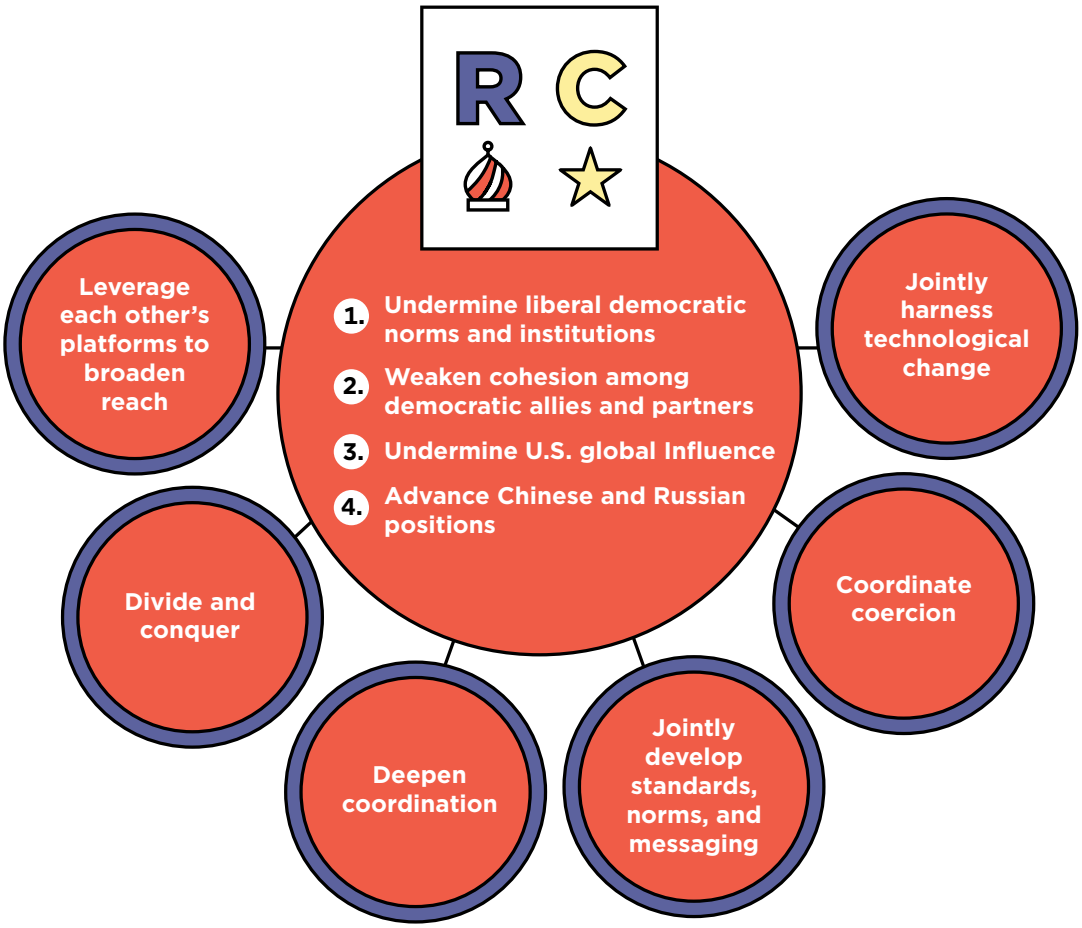
Forecasting China-Russia Synergies

Looking forward, the coordination and resulting synergy between China and Russia in the informational domain is likely to grow. Already, there is an expanding body of evidence demonstrating their growing ties in areas related to digital influence. These ties will provide a foundation for greater cooperation and coordination, increasing the challenges that the United States and other liberal democracies will face in the information environment.

Deepening Coordination

China and Russia are increasing their coordination on issues related to digital influence, ranging from cybersecurity and cyberspace to broadcast and online media. Their shared threat perception and mutual interests have led to a number of agreements and initiatives. In the cybersecurity realm, for example, Xi and Putin signed an agreement in 2015 to work together to ensure international information security. Since the agreement was signed, China and Russia have conducted a number of exchanges designed to share technologies, information, and processes to control the internet. Likewise, continued Russia-China collaboration at the U.N. on issues such as cybercrime have provided an additional vehicle to work together in an attempt to create U.N.-approved standards for controlling the flow of information.

Beijing and Moscow have also sought to institutionalize cooperation in conventional broadcast and online media. The two countries have in recent years established various knowledge-sharing mechanisms, including the China-Russia Media Forum. On the sidelines of the 2019 Eastern Economic Forum in Vladivostok, the two countries held their fifth installment of the China-Russia Media Forum, which brought



Looking forward, the coordination and resulting synergy between China and Russia in the informational domain is likely to grow. These ties will provide a foundation for greater cooperation, increasing the challenges that the United States and liberal democracies will face in the information environment.

together representatives from their respective media outlets, internet platforms, and other relevant industries to spur discussion around content and data sharing, digital media collaboration and "strengthening the standing of Chinese and Russian media in global markets."[127] And at the third China-Russia Internet Media Forum in November 2019, Yang Xiaowei, deputy director of the Cyberspace Administration of China, hailed the deepening ties between Russian and Chinese media while his counterpart Alexey Volin, Russia's deputy minister of digital development, communications, and mass media, discussed the importance of advancing cooperation in new frontiers of online communications and entertainment industries, including movies, television programming, and gaming.[128]

As the exchange of best practices and cross-border learning of tactics becomes increasingly hard-wired into the interactions between China and Russia, the CCP and the Kremlin are positioned to deepen coordination on digital influence. These habits of cooperation are poised to become more problematic for democracies as both China and Russia seek to improve their capacity to advance their own narratives globally—an objective that the CCP characterizes as "discourse power."[129] Looking forward, China and Russia could leverage their comparative strengths to weaken the perceived Western-dominated global information environment while setting forth alternative platforms—and corresponding norms—by which information can be disseminated.

Dividing and Conquering

While Russian efforts remain focused on weakening and dividing democratic societies in Europe and the United States, China is spreading the tentacles of its online influence campaigns in strategically positioned developing countries across Southeast Asia, Central Asia, Latin America, and Africa. Chinese media companies such as StarTimes have, for example, have expanded their equities in the digital television broadcasting sector, particularly targeting emerging markets using enticing, low-cost package offerings to audiences in countries such as Kenya, Uganda, and Nigeria—or through forming joint ventures with local or national television stations.[130] Meanwhile, Moscow remains willing and well positioned to do Beijing's bidding when it comes to promoting Chinese media products, telecommunications infrastructure, and other technology in countries across Europe and other Western countries, particularly if this bestows the two countries with additional levers by which to curtail the spread of the free information apparatus

Russian President Vladimir Putin addresses the plenary session of the Eastern Economic Forum in 2019. On the sidelines of the 2019 Eastern Economic Forum in Vladivostok, Russia and China held their fifth installment of the China-Russia Media Forum as part of an effort to institutionalize cooperation in conventional broadcast and online media. (President of Russia/The Kremlin)

China and Russia are together exerting both internal and external pressure on open societies by compromising the integrity of existing platforms while seeking to undercut the perceived Western monopoly on the global information ecosystem.

that democracies seek to promote.[131] In addition to this regional division of labor, there is a tactical battle rhythm that is emerging between China and Russia as well. For example, while Russia primarily propagates divisive content on pre-existing and well-established platforms—such as Western social media sites and Moscow-based broadcast media—China is ever more focused on developing entirely new platforms by which to disseminate information. In doing so, China and Russia are together exerting both internal and external pressure on open societies by compromising the integrity of existing platforms while seeking to undercut the perceived Western monopoly on the global information ecosystem.

Leveraging Each Other's Platforms to Broaden Reach

Likewise, the proliferation of popular Chinese-designed and -marketed social media apps that run parallel to Western platforms has the potential to create entirely alternative information ecosystems that China and Russia could jointly leverage. Indeed, as Chinese apps multiply globally, the CCP's information operations can move more nimbly and covertly in democratic societies. Chinese state actors have, for example, used WeChat to mobilize the Chinese diaspora to take to polling stations during Canada's 2019 federal election, which potentially foreshadows how the CCP might leverage WeChat for more direct influence in future democratic elections.[132] If WeChat and other Chinese-designed apps prove to be effective vehicles for shaping the preferences of the Chinese diaspora, Russia might turn to these platforms as well to amplify polarizing and destabilizing messages in the United States or other Western societies.

In the traditional and broadcast media space, the *Global Times*—one of China's major media outlets under the auspices of the CCP's *People's Daily* newspaper—already announced in 2017 a partnership with Russia's Sputnik news agency, bumping Sputnik's total number of contracts with large Chinese media organizations, including Xinhua and China Radio International, up to eight.[133] By virtue of these agreements, Beijing-friendly content has proliferated in Russian outlets, while Chinese news services have similarly taken up the mantle of promoting Russia's informational agenda.

Jointly Harnessing Technological Change

As Beijing and Moscow move to shape the global information environment both independently and jointly through the wide range of tools discussed in the previous sections, their exchange of best practices and mutual learning around these tools will migrate to cutting-edge capabilities that are difficult to detect but yield maximal payoff in eroding democratic institutions globally. For example, a major area of focus for Chinese and Russian investments in next-generation digital interference capabilities will include controlling the platforms, software, and manner in which day-to-day activities are conducted online.

Existing Chinese- and Russian-designed apps have already generated risks to democratic societies, but as they gain traction, their virality would ensure that they move more quickly than governments' ability to confirm or deny their verity. Chinese apps that allow users to create low-quality deep fakes in mass quantities—such as Zao, Yanji, and a pending feature within TikTok dubbed "Face Swap"—have proliferated since 2019.[134] And the photo-transforming FaceApp that went viral as the most-downloaded smartphone app in the United States in the summer of 2019 caused disarray after it was revealed that a relatively unknown Russian firm had developed the app.[135] By taking advantage of opaque ownership structures, front companies, and flimsy assurances about data security practices, China and Russia are increasingly well positioned to pilot viral apps that use artificial intelligence and natural language processing software to collect, analyze, and generate data that erodes public faith and understanding of the idea of truth.[136]

Finally, technological change will also have the potential to enhance and enable the widespread use of tools such as microtargeting and deep fakes that Russia and China can harness to more effectively manipulate the information environment. Although the two countries would be unlikely to directly coordinate their employment of such tools, their ability to learn lessons and best practices from each other could accelerate their effective use of these methods.

Coordinating Coercion

Concerns around data harvesting associated with Chinese apps have grown acute, particularly among political activists critical of Beijing's policies and in countries suspicious of China's geopolitical ambitions. As both Beijing and Moscow look to silence dissidents in online spaces, concrete collaboration between the CCP and Russian actors could become more of an attractive option for both countries. While evidence of collaboration largely remains circumstantial at present, Beijing and Moscow are certainly positioned to leverage each other's technology to try to silence dissent. In 2019, for example, CCP organs harvested the personal information of protesters in Hong Kong from their social media profiles and other databases and publicly released their personal data on social media and websites including HK Leaks, which was notably hosted on a Russian domain.[137] Societies that rely on Chinese apps, such as social media or e-payment platforms run by Tencent, to conduct day-to-day activities are uniquely vulnerable to coordinated coercion, as state actors could leverage data grafted from these platforms to shape behavior in ways that align with their interests.

Jointly Developing Norms and Messaging

Already, executives from China's *People's Daily* and Russia's *Rossiyskaya Gazeta* who attended the media forum in 2019 have advocated for coordinating more closely to fend off "twisted and biased coverage" from Western outlets.[138] Beijing, all the while, showcases the success of its own domestic model of information control and management by conducting large-scale trainings of foreign officials on managing public opinion and new media.[139] By developing the rails and pipelines of an alternative information infrastructure, China and Russia are positioned to jointly promulgate a vision of a digital order shaped by the preferences of authoritarian states.

As China and Russia compete more broadly with democracies over the future of the global information space, they will seek to create a sense of moral equivalency to the United States' democracy promotion activities dating back to the height of the Cold War. Chinese and Russian diplomats are likely to continue to try to flip the script and cast blame on the United States for meddling in their internal affairs while contending that Beijing and Moscow are seeking to "democratize" the information space by popularizing non-Western news media, social media, and other online platforms. Both countries, for example, have blamed the United States for interfering in their internal affairs amid flare-ups of political movements, most notably in Hong Kong in 2019. Absent clear and shared guidelines advanced by democracies to underscore how the Chinese and Russian activities are fundamentally different, these illiberal actors are increasingly well positioned to blur these moral boundaries.

By developing the rails and pipelines of an alternative information infrastructure, China and Russia are positioned to jointly promulgate a vision of a digital order shaped by the preferences of authoritarian states.

Recommendations

The United States and its democratic allies and partners should adopt a holistic approach to countering digital influence campaigns by China and Russia, particularly in light of the growing synergies between these two powers. This approach must strike the right balance between minimizing opportunities for authoritarian interference and sustaining the open information ecosystems that remain critical to economic prosperity and democratic governance. It should also move beyond a tactical focus and instead seek to address information ecosystems as a whole, starting with individual users, scaling up to social media platforms, and extending to relevant international legal and normative frameworks.[140] Lastly, the United States and its democratic allies and partners should develop and implement cost imposing measures to deter future digital influence campaigns by China and Russia.

In practice, this approach should comprise four primary lines of effort: bolstering democratic resilience to digital influence campaigns; enhancing coordination among targeted democracies; constructing and sustaining healthy information ecosystems; and imposing costs to build a new form of deterrence. Below are concrete and actionable recommendations for advancing each line of effort. Collectively, these recommendations would enable the United States and its democratic allies and partners to address the most pernicious forms of authoritarian digital interference: meddling in elections, promoting polarization, and inculcating pro-China and pro-Russia narratives.

Bolster Resilience to Digital Influence Campaigns

Fund targeted open source research. Scholars at universities and think tanks have in recent years dedicated significant attention to Chinese and Russian digital influence campaigns.[141] However, despite an extensive body of intellectual work, several analytic gaps exist. Detailed case studies of China-Russia coordination remain limited, even as evidence mounts of growing synergies between the two. Moreover, rigorous research efforts to understand the effects of authoritarian digital influence campaigns on the perceptions of citizens in democracies—i.e., what tactics actually succeed in shaping views—remain nascent. Addressing these analytic gaps is a prerequisite to helping policymakers prioritize the problem and enacting policy responses that bolster democratic resiliency to digital influence campaigns by both China and Russia. Accordingly, the National Science Foundation should ramp up funding for social science research in these two areas.

These recommendations would enable the United States and its democratic allies and partners to address the most pernicious forms of authoritarian digital interference: meddling in elections, promoting polarization, and inculcating pro-China and pro-Russia narratives.

Expand digital literacy education to adults. Democracies such as Taiwan and Finland have systematically introduced digital literacy curriculums into their classrooms to help inoculate students against digital influence campaigns by their authoritarian neighbors.[142] Meanwhile, in the United States, digital literacy remains a patchwork effort, with education companies and leading information technology firms putting forward their own curriculums geared toward students.[143] This focus on the rising generation is critical but overlooks voting-age citizens, including the elderly, who are particularly prone to sharing false information online.[144] The U.S. Department of Education should partner with a leading information technology company to design a user-friendly digital citizenship course for American adults. The course would be accessible online and through a downloadable cellphone app. To incentivize Americans to enroll in the course and take a refresher each year, the U.S. government could offer a small tax rebate for annual completion. This model, if successful, could be replicated across other democracies, though the incentive scheme for enrollment might differ.

Regulate the social media landscape.[145] Recognizing that each social media app is unique, the United States can nonetheless take several general steps to better secure these platforms against digital influence campaigns by China and Russia. First, Congress should enact legislation mandating that social media companies label content disseminated by state-sponsored actors. This would help users to determine the veracity and agenda behind such content.[146] Second, Congress should pass legislation requiring social media companies to share with trusted researchers data on digital influence campaigns by authoritarian states. Enhanced information sharing by social media platforms would bolster the

expert community's ability to analyze online interference activities by China and Russia. Third, Congress should urge social media companies to voluntarily downgrade in their algorithms content emanating from state-controlled outlets in authoritarian countries (i.e., Xinhua News Agency and Russia Today), while refraining from heavy-handed legislation that would inadvertently mimic the types of content controls put in place by authoritarian states.[147]

Expand Coordination among Democracies

Red team China-Russia synergies. Efforts by China and Russia to coordinate their digital influence campaigns and learn from each other should concern American allies in Europe and the Indo-Pacific. Now is the time for the United States to invite its democratic allies from both regions to come together, share perspectives, and explore how the world's two leading authoritarian powers might ramp up cooperation in the digital domain in order to shape election outcomes, fuel polarization, and promote favorable narratives. Intended to red team future China-Russia synergies, this convening would bring together intelligence analysts, diplomats, domestic security specialists, and technologists from the United States, Europe, Japan, Taiwan, and Australia.

Stress-test existing coordination structures. In recent years, the United States and other economically advanced democracies have launched new coordination mechanisms to combat authoritarian influence campaigns, often with a particular focus on the digital domain. Prominent examples include the Group of Seven (G7) Rapid Response Mechanism and the European Union's Rapid Alert System.[148] Largely below the radar, the Five Eyes intelligence alliance has reportedly enhanced cooperation with a handful of democracies such as Germany and Japan to counter foreign interference emanating from China.[149] Real-time intelligence sharing through such mechanisms is a prerequisite for the United States and its democratic allies and partners to mount a collective and coherent response to authoritarian digital influence campaigns. Recognizing that speed is critical, the United States, initially through the G7 Rapid Response Mechanism, should conduct an intelligence sharing exercise that would identify bottlenecks in current arrangements for disseminating classified information. Based on the findings of this exercise, the United States and other members of the G7 could put in place new processes for timely intelligence sharing.

Leverage the Community of Democracies. A critical weak point in the current international architecture for combating Chinese and Russian digital influence campaigns is the exclusion of developing countries from the most prominent coordination mechanisms, even though they are also potential targets. The United States should advance a new and more inclusive coordination mechanism, leveraging the Community of Democracies (CoD)—a global intergovernmental coalition with a membership spanning Latin America, Africa, and developing Asia.[150] Recognizing that CoD members have diverse views of China and Russia, the United States should couch the new coordination mechanism in broad terms of countering foreign interference, with a focus on the digital domain. In its early stages, the coordination mechanism would provide an opportunity to share unclassified information and facilitate an exchange of best practices for inoculating democracies against externally orchestrated digital influence campaigns.

Act in concert with other democracies in international organizations. The United States should work with its democratic allies and partners to advance an agenda in international forums that delegitimizes online influence campaigns by China and Russia and mitigates their potential impact. This starts by joining the more than 50 countries that have already signed the Paris Call for Trust and Security in Cyberspace. Although not legally binding, this agreement advances norms against election interference.[151] Set against the larger backdrop of current U.S. antipathy toward multilateralism, America's absence from the Paris Call erodes its ability to muster international support for addressing Chinese and Russian digital influence campaigns more generally. Beyond reinforcing international norms, the United States should work with its democratic allies and partners at the United Nations to link digital citizenship—with an emphasis on education geared toward inoculating populations against online manipulation—to the 2030 Sustainable Development Goals (SDGs). Linkage to the SDGs could provide momentum for funneling U.N. resources toward programs intended to build digital literacy across the developing world, with the intent of empowering populations to identify false information and inorganic content amplification. Lastly, at the U.N. and in other relevant multilateral organizations, Washington and like-minded democratic capitals should advance access to fact-based information as a universal human right—drawing a sharp contrast with the government-curated information ecosystems of authoritarian powers such as China and Russia.[152]

Construct and Sustain Healthy Information Ecosystems

Support independent diaspora media. Beijing and Moscow have respectively sought to mobilize Chinese- and Russian-language diasporas through a variety of instruments, including digital influence campaigns.[153] Given the role these diasporas play within U.S. allies in Eastern Europe and Asia, ensuring that these populations have access to credible and independent information sources in their home languages should be a priority for the United States. In recent years, Washington under the umbrella of the U.S. Agency for Global Media (formerly the Broadcasting Board of Governors) has dedicated increased funding and resources toward engaging with Chinese- and Russian-language diasporas. For example, Radio Free Europe in 2017 inaugurated a 24-hour Russian television channel, and Radio Free Asia has partnered with Voice of America to launch an initiative aimed at "young Mandarin-speaking audience around the world."[154] The United States should double down on these efforts, while also empowering media indigenous to the Chinese- and Russian-language diasporas. For example, the State Department could partner with a highly credible nongovernmental organization such as the International Center for Journalists to award grants to Chinese- and Russian-language reporters and media entrepreneurs, based on selection criteria that elevate a local connection and independence from Beijing and Moscow.

Subsidize fact-based content in regions where affordability matters most. In developing countries, pricing can play a critical role in determining what sources populations turn to for information. Beijing in particular has made a concerted effort to shape the information ecosystems of developing countries by offering free content to local providers and supporting on-the-ground activities by Chinese media companies, such as converting households from analog to digital television.[155] The United States can do more to bring down the cost of fact-based content in developing countries. It should offer to subsidize the cost to local media outlets of maintaining a subscription to The Associated Press wire service—an approach that has proved successful when road tested in the Pacific Islands. In addition, the new U.S. International Development Finance Corporation should pursue opportunities to extend loans and other supports to American media companies looking to grow their presence in developing markets.

Catalyze innovative technological solutions. Technology can play an important role in enabling democracies to safeguard their information ecosystems against digital influence campaigns by China and Russia. However, what commercial markets currently provide is limited. The United States should galvanize innovation to develop scalable solutions. This could begin with the Defense Advanced Research Projects Agency (DARPA) organizing a "Democratic Integrity Hackathon" that would bring together engineers and entrepreneurs to develop products to protect social media platforms against current and especially future instances of Chinese and Russian digital influence campaigns.[156] A primary focus would be on countering the use of graphics and video to shape public perceptions in democracies—mediums more challenging to identify and analyze than text.[157] Leveraging resources allocated to the Global Engagement Center at the State Department, the United States could finance the most promising concepts generated by the hackathon, ideally augmented by funding from interested foundations and venture capitalists.

Enhance Efforts to Deter China and Russia

Develop a menu for cost imposition. Beyond bolstering resilience, expanding international coordination, and constructing and sustaining healthy information ecosystems, the United States and its democratic allies and partners should develop a robust set of options to impose costs on China and Russia, with the aim of deterring the most egregious forms of digital influence campaigns. These actions would be most likely to deter Russian and Chinese actions if articulated clearly, and in advance. These options, listed in ascending order of escalatory risk, include the following:

- Demonstrate an ability to hold at risk sensitive personal data of Chinese or Russian senior leadership in response to state-sponsored digital influence campaigns.[158]
- Direct Global Magnitsky Act sanctions against actors from China or Russia responsible for orchestrating digital influence campaigns.[159]
- Scale up efforts to disseminate tools to internet users in China or Russia that enable avoidance of online monitoring and censorship and help to identify inorganic content amplification.
- Suspend leader-level summits and expel the ambassador in Washington after Chinese or Russian state-sponsored digital influence campaigns that cross pre-specified disruptive thresholds, such as hacking and leaking sensitive political information prior to an election.

- Inject fact-based information into the online ecosystem of China or Russia that exposes the corruption of their elites and larger flaws of their authoritarian systems.

Establish a declaratory policy. Although it will be impossible to deter all forms of Chinese and Russian digital influence activities, the above options—if coupled with a declaratory policy—could at least give Beijing and Moscow pause. The United States should quietly convey to both that it is willing and able to impose costs, particularly with respect to online interference that touches on election integrity.[160]

Use costs imposed on Russia to warn and deter China. Ultimately, Moscow is considerably more risk acceptant than Beijing, and likely to engage in types of digital interference that cross American thresholds for cost imposition. Such circumstances present an opportunity to reinforce deterrence vis-à-vis China, which though learning from Russia, remains more risk averse. In parallel with punishing Russia, American policymakers should privately communicate to Beijing that they could exercise similar options against it, but have exercised restraint, due to China's less aggressive behavior.

These recommendations would enable the United States and its democratic allies and partners to address the most pernicious forms of authoritarian digital interference: meddling in elections, promoting polarization, and inculcating pro-China and pro-Russia narratives.

Conclusion

The contest to shape the global information environment is arguably the most important domain of the political, ideological, and broader strategic competition between the United States and leading authoritarian states, namely China and Russia. But while Beijing and Moscow have invested considerable institutional wherewithal and strategic focus to mobilizing their online information operations through increasingly covert and sophisticated means, the United States has largely been caught on the back foot. Both individually and jointly, Beijing and Moscow are leveraging their countries' technological and media resources to diminish the United States' global influence and to advance their own geopolitical aims—and the gravitational pull of these symbiotic approaches is only likely to grow stronger. Through an increasingly diverse and technologically advanced toolkit—ranging from astroturfing and targeted online advertising to deep fakes and viral social media apps—both China and Russia are able to mobilize their online campaigns more nimbly and covertly to gain a foothold in societies around the world and to diminish the United States' global influence.

The United States must, therefore, not only continue to step up defensive efforts in the near term but should also leverage its clout in international forums to move offensively—in close coordination with democratic allies and partners—to deter and delegitimize the most egregious of Chinese and Russian online influence campaigns. Ultimately, the openness of American online platforms and the broader information environments of democracies remains a vital asset, particularly when contrasted with the opacity and impermeability of Beijing's and Moscow's domestic information spaces.[161] The beginning and end of U.S. efforts to promote resilience, both at home and abroad, should ultimately be to equip publics with a precise understanding of how Beijing and Moscow are leveraging online platforms to censor, surveil, and erode truth amid their informational contest with the United States.

Lastly, to win the informational contest with China and Russia, the United States must broadly reassert its international leadership. An America that galvanizes global coalitions to rise to common challenges will render Beijing's and Moscow's digital influence operations against U.S. allies and partners less effective. Conversely, an inward-looking United States will create fertile ground for China and Moscow to continue their synergistic efforts to bend the global information landscape to their joint advantage.[162]

1. Andrea Kendall-Taylor and David Shullman, "How Russia and China Undermine Democracy: Can the West Counter the Threat?" *Foreign Affairs,* October 2, 2018, https://www.foreignaffairs.com/articles/china/2018-10-02/how-russia-and-china-undermine-democracy?cid=int-lea&pgtype=hpg.

2. An earlier variant of this recommendation was first put forward by Kristine Lee and Karina Barbesino, "Challenging China's Bid for App Dominance" (Center for a New American Security, January 22, 2020), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-HTI-App-Dominance-DoSproof.pdf?mtime=20200121212333.

3. Bethany Allen-Ebrahimian, "China steps up political interference ahead of Taiwan's elections," Axios, January 10, 2020, https://www.axios.com/china-disinformation-taiwan-presidential-election-0f66ae16-0140-4c84-a833-bf5653cecf85.html; and Joshua Kurlantzick, "How China Is Interfering in Taiwan's Election," Council on Foreign Relations, November 7, 2019, https://www.cfr.org/in-brief/how-china-interfering-taiwans-election.

4. "Freedom in the World 2019: Democracy in Retreat," (Freedom House, 2019), https://freedomhouse.org/report/freedom-world/2019/democracy-retreat.

5. Christina Nemr and William Gangware, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age" (Park Advisors, March 2019), https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

6. Jamie Fly, Laura Rosenberger, and David Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies" (The German Marshall Fund of the United States, June 26, 2018), http://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies.

7. Only 47 percent of citizens trusted their governments worldwide in 2019. Edelman Intelligence, "2019 Edelman Trust Barometer: Global Report," https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Global_Report_2.pdf.

8. Fly, Rosenberger, and Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies"; and Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D (January 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

9. Sarah Repucci, "Freedom and the Media: A Downward Spiral" (Freedom House, 2019), https://freedomhouse.org/sites/default/files/2020-02/FINAL07162019_Freedom_And_The_Media_2019_Report.pdf.

10. President of the Russian Federation, "The Military Doctrine of the Russian Federation" (in Russian), February 5, 2010, https://web.archive.org/web/20110504070127/http://www.scrf.gov.ru/documents/33.html, accessed November 2019.

11. Elizabeth Bodine-Baron et al., "Countering Russian Social Media Influence" (RAND Corp., 2018), https://www.rand.org/pubs/research_reports/RR2740.html.

12. Mark Galeotti, "Controlling Chaos: How Russia manages its political war in Europe" (European Council on Foreign Relations, September 1, 2017), https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

13. Liu Yunshan, "回顾与展望 [Seeking Truth: Review and Outlook]," QSTheory, June 22, 2009, http://www.qstheory.cn/zxdk/2009/200901/200906/t20090609_1625.htm.

14. Anne-Marie Brady, "Authoritarianism Goes Global (II): China's Foreign Propaganda Machine," *Journal of Democracy*, 26 no. 4 (October 2015), 51-59, https://www.journalofdemocracy.org/articles/authoritarianism-goes-global-ii-chinas-foreign-propaganda-machine/.

15. "把网上舆论工作作为宣传思想工作的重中之重 [Make online public opinion work the top priority of propaganda and ideological work]," CPCNews, October 31, 2013, http://theory.people.com.cn/n/2013/1031/c40537-23387807.html.

16. Damien Ma and Neil Thomas, "In Xi We Trust: How Propaganda Might Be Working in the New Era," MacroPolo, September 12, 2018, https://macropolo.org/analysis/in-xi-we-trust/.

17. Peter Harrell, Elizabeth Rosenberg, Edoardo Saravalle, "China's Use of Coercive Economic Measures" (Center for a New American Security, June 11, 2018), https://s3.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240; Ben Blanchard and Andrew Heavens, "U.S. 'smears' of China affecting global stability, top Beijing diplomat says," Reuters, December 23, 2019, https://www.reuters.com/article/us-china-usa/u-s-smears-of-china-affecting-global-stability-top-beijing-diplomat-says-idUSKBN1YR1I4.

18. "Chinese Influence & American Interests: Promoting Constructive Vigilance" (Hoover Institution, 2018), https://www.hoover.org/sites/default/files/research/docs/chineseinfluence_americaninterests_fullreport_web.pdf; and Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, and James Sladden, "Hostile Social Manipulation: Present Realities and Emerging Trends," (RAND Corp., 2019), https://www.rand.org/pubs/research_reports/RR2713.html.

19. Ministry of National Defense, *China's Military Strategy*, May 26, 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.; The State Council, *China's National Defense in the New Era*, July 24, 2019, http://english.www.gov.cn/archive/whitepaper.

20. "Moscow calls for joint cooperation with Beijing against U.S. interference," Xinhua, August 9, 2019, http://www.xinhuanet.com/english/2019-08/09/c_138297092.htm.

21. Gideon Rose, "Is Democracy Dying?," *Foreign Affairs* (May/June 2018), https://www.foreignaffairs.com/articles/2018-04-16/democracy-dying.

22. Miles Maochun Yu, "China's Strategic Ambiguity," Hoover Institution, June 25, 2018, https://www.hoover.org/research/chinas-strategic-ambiguity.

23. Agnieszka Legucka, "Russia's Long-Term Campaign of Disinformation in Europe," Carnegie Europe, March 19, 2020, https://carnegieeurope.eu/strategiceurope/81322.

24. Legucka, "Russia's Long-Term Campaign of Disinformation in Europe."

25. Thomas Grove, "Russia Gives China a Leg Up in Foreign Broadcasting," *The Wall Street Journal*, January 14, 2020, https://www.wsj.com/articles/russia-gives-china-a-leg-up-in-foreign-broadcasting-11579003202.

26. Jessica Brandt and Torrey Taussig, "Europe's Authoritarian Challenge," *The Washington Quarterly,* Winter 2020, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2019/12/BrandtTaussig_42-4.pdf?

27. Echo Huang, "Why China isn't as skillful at disinformation as Russia," Quartz, September 18, 2019, https://qz.com/1699144/why-chinas-social-media-propaganda-isnt-as-good-as-russias/.

28. Blanchard and Heavens, "U.S. 'smears' of China affecting global stability, top Beijing diplomat says"; and Javier C. Hernández, "China Spins Coronavirus Crisis, Hailing Itself as a Global Leader," *The New York Times*, February 28, 2020, https://www.nytimes.com/2020/02/28/world/asia/china-coronavirus-response-propaganda.html.

29. Anton Troianovski, "Russa Savors U.S. Missteps in Syria, and Seizes Opportunity," *The New York Times*, October 14, 2019, https://www.nytimes.com/2019/10/14/world/europe/russia-savors-us-missteps-in-syria-and-seizes-opportunity.html.

30. Anna Borshchevskaya and Catherine Cleveland, "Russia's Arabic Propaganda" (Washington Institute for Near East Policy, December 2018), https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyNote57-BorshchevskayaCleveland.pdf.

31. Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion," Recorded Future, March 6, 2019, https://www.recordedfuture.com/china-social-media-operations/.

32. Clarissa Ward, Katie Polglase, Sebastian Shukla, Gianluca Mezzofiore, and Tim Lister, "Russian election meddling is back – via Ghana and Nigeria – and in your feeds," CNN, March 13, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html.

33. Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion."

34. Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument," *American Political Science Review* (April 9, 2017), 111, http://gking.harvard.edu/files/gking/files/50c.pdf?m=1463587807&version=meter+at+0&module=meterLinks&pgtype=article&contentId=&mediaId=&referrer=&priority=true&action=click&contentCollection=meter-links-click.

35. Cao Desheng, "Xi's discourses on mankind's shared future published," *China Daily*, October 15, 2018, http://www.chinadaily.com.cn/a/201810/15/WS5bc38adca310eff303282392.html.

36. Tom Uren, Elise Thomas, and Dr. Jacob Wallis, "Tweeting through the Great Firewall" (Australian Strategic Policy Institute, September 3, 2019), https://www.aspi.org.au/report/tweeting-through-great-firewall.

37. The authors are indebted to commentary by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security for some of the insights contained in this subsection.

38. Jessica Brandt and Torrey Taussig, "Europe's Authoritarian Challenge," *The Washington Quarterly,* Winter 2020, https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2019/12/BrandtTaussig_42-4.pdf?

39. Jack Nicas, "Apple Removes App That Helps Hong Kong Protesters Track the Police," *The New York Times,* October 9, 2019, https://www.nytimes.com/2019/10/09/technology/apple-hong-kong-app.html.

40. Mark Gurman, "Apple Pulls Taiwanese Flag Emoji From iPhones in Hong Kong," Bloomberg, October 8, 2019, https://www.bloomberg.com/news/articles/2019-10-08/apple-pulls-taiwanese-flag-emoji-from-iphones-in-hong-kong.

41. Harry Krejsa, "Under Pressure: The Growing Reach of Chinese Influence Campaigns in Democratic Societies" (Center for a New American Security, April 2018), https://www.cnas.org/publications/reports/under-pressure; Paige Leskin, "Here are all the major US tech companies blocked behind China's 'Great Firewall,'" Business Insider, October 10, 2019, https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5#google-2.

42. "Top Apps Worldwide for Q1 2019 by Downloads," Sensor Tower Blog on SensorTower.com, May 15, 2019, https://sensortower.com/blog/top-apps-worldwide-q1-2019-downloads; Geoffrey Gertz, "Is TikTok a threat to national security?" *The Washington Post*, November 11, 2019, https://www.washingtonpost.com/politics/2019/11/11/is-tiktok-threat-national-security/.

43. Tamara Khandaker, "The WeChat factor," Vice, February 1, 2019, https://www.vice.com/en_ca/article/zmana5/experts-say-we-should-watch-out-for-wechats-influence-in-canadas-election.

44. Isobel Asher Hamilton, "WeChat users in the US say the app is censoring their messages about Hong Kong," Business Insider, November 26, 2019, https://www.businessinsider.com/us-wechat-users-censored-messages-hong-kong-china-2019-11.

45. Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model" (RAND Corp., 2016), https://www.rand.org/pubs/perspectives/PE198.html.

46. Henry Farrell and Bruce Schneier, "Democracy's Dilemma," Boston Review, May 15, 2019, https://bostonreview.net/forum-henry-farrell-bruce-schneier-democracys-dilemma.

47. Seva Gunitsky, "The Great Online Convergence: Digital Authoritarianism Comes to Democracies," War on the Rocks, February 19, 2020, https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/.

48. Mark Urban, "Skripal poisoning: Third Russian suspect 'commanded attack,'" BBC, June 28, 2019, https://www.bbc.com/news/uk-48801205.

49. Jane Li, "Russia is Beijing's best ally in the disinformation war against Hong Kong," Quartz, December 11, 2019, https://qz.com/1765092/russia-is-beijings-ally-in-media-war-against-hong-kong/.

50. Hua Chunying, "Hua Chunying zai xuexi shibao zhuanwen: zhanju daoyi zhi gao dian, tisheng guoji huayu quan [Hua Chunying in a Study Times article: Occupy the moral high ground and enhance our international voice]," Pengpai Xinwen, July 12, 2019, https://www.thepaper.cn/newsDetail_forward_3900567.

51. Raymond Zhong, "Awash in Disinformation Before Vote, Taiwan Points Finger at China," *The New York Times*, January 6, 2020, https://www.nytimes.com/2020/01/06/technology/taiwan-election-china-disinformation.html.

52. Adam Taylor, "China's Foreign Ministry adopts a Trumpian tone on its new Twitter account – with insults, typos, ALL-CAPS and emoji," *The Washington Post*, December 5, 2019, https://www.washingtonpost.com/world/2019/12/05/chinas-foreign-ministry-adopts-trumpian-tone-its-new-twitter-account-with-insults-typos-all-caps-emojis/.

53. Josh Rogin, "China's interference in the 2018 elections succeeded – in Taiwan," December 18, 2018, *The Washington Post*, https://www.washingtonpost.com/opinions/2018/12/18/chinas-interference-elections-succeeded-taiwan/.

54. Lihyun Lin, "Digital News Report: Taiwan," Reuters Institute and University of Oxford, March 2018, http://www.digitalnewsreport.org/survey/2018/taiwan-2018/.

55. Matthew Strong, "Taiwan Legislative Yuan approves Anti-Infiltration Act aimed at China," TaiwanNews.com, December 31, 2019, https://www.taiwannews.com.tw/en/news/3847852; and Connor Fairman, "When Election Interference Fails," Council on Foreign Relations' Net Politics blog on CFR.org, January 29, 2020, https://www.cfr.org/blog/when-election-interference-fails.

56. Kate Conger, "Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong," *The New York Times*, August 19, 2019, https://www.nytimes.com/2019/08/19/technology/hong-kong-protests-china-disinformation-facebook-twitter.html; and Editorial Board, "China is copying Russia's Internet attacks. It's good that Twitter and Facebook responded," *The Washington Post*, August 21, 2019, https://www.washingtonpost.com/opinions/global-opinions/china-is-copying-russias-internet-attacks-its-good-that-twitter-and-facebook-responded/2019/08/21/979d3e22-c433-11e9-b5e4-54aa56d5b7ce_story.html.

57. Unofficially known as the 50 Cent Army because of early allegations that employees would be paid 0.50 yuan per post, these bots consist of individuals hired by CCP authorities to generate, disseminate, and enforce pro-Beijing narratives online in an attempt to manipulate public opinion to benefit the CCP.

58. Craig Timberg, Drew Harwell, and Tony Romm, "In accusing China of disinformation, Twitter and Facebook take on a role they've long rejected," *The Washington Post*, August 20, 2019, https://www.washingtonpost.com/technology/2019/08/20/after-twitter-facebook-blame-china-hong-kong-disinformation-government-defends-its-right-online-speech/.

59. Samantha Bradshaw and Phillip N. Howard, "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life" (Knight Foundation, January 29, 2018), 12-13, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

60. Nemr and Gangware, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age."

61. Paresh Dave and Katie Paul, "Facebook defies China headwinds with new ad sales push," Reuters, January 7, 2020, https://www.reuters.com/article/us-facebook-china-focus/facebook-defies-china-headwinds-with-new-ad-sales-push-idUSKBN1Z616Q.

62. Isobel Asher Hamilton, "Facebook took down a bunch of political Huawei adverts in the latest blow to the Chinese tech firm," Business Insider, June 17, 2019, https://www.businessinsider.com/facebook-takes-down-huawei-adverts-2019-6; and Janhvi Bhojwani, "Huawei Broadens Its Campaign To Win Over American Public And Media," NPR, March 1, 2019, https://www.npr.org/2019/03/01/699307312/huawei-broadens-its-campaign-to-win-over-american-public-and-media.

63. Dan Levin, "Chinese-Canadians Fear China's Rising Clout is Muzzling Them," *The New York Times*, August 27, 2016, https://www.nytimes.com/2016/08/28/world/americas/chinese-canadians-china-speech.html.

64. Tony Romm, "'Pro-Beyoncé' vs. 'Anti-Beyoncé': 3,500 Facebook ads show the scale of Russian manipulation," *The Washington Post*, May 10, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/10/here-are-the-3400-facebook-ads-purchased-by-russias-online-trolls-during-the-2016-election/.

65. Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *The New York Times*, November 1, 2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

66. Maria Snegovaya, "Russian Propaganda In Germany: More Effective Than You Think," *The American Interest* (October 17, 2017), https://www.the-american-interest.com/2017/10/17/russian-propaganda-germany-effective-think/.

67. Philip Oltermann and Rina Soloveitchik, "How Germany's Russian minority could boost far right," *The Guardian*, September 22, 2017, https://www.theguardian.com/world/2017/sep/22/how-germanys-russian-minority-could-boost-far-right; and Stefan Meister, "The 'Lisa case': Germany as a target of Russian disinformation," NATO Review, July 25, 2016, https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

68. "List of Sector Members," International Telecommunication Union, https://www.itu.int/online/mm/scripts/gensel11.

69. Danielle Cave, Dr. Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants" (Australian Strategic Policy Institute, April 18, 2019), https://www.aspi.org.au/report/mapping-chinas-tech-giants; and Kristine Lee and Alexander Sullivan, "People's Republic of the United Nations" (Center for a New American Security, May 14, 2019), https://www.cnas.org/publications/reports/peoples-republic-of-the-united-nations.

70. Yimou Lee and I-hwa Cheng, "Paid 'news': China using Taiwan media to win hearts and minds on island – sources," Reuters, August 9, 2019, https://www.reuters.com/article/us-taiwan-china-media-insight/paid-news-china-using-taiwan-media-to-win-hearts-and-minds-on-island-sources-idUSKCN1UZ0I4; and Rush Doshi, "China Steps Up Its Information War in Taiwan," *Foreign Affairs* (January 9, 2020), https://www.foreignaffairs.com/articles/china/2020-01-09/china-steps-its-information-war-taiwan.

71. Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn, "Disinformation Warfare: Understanding State-Sponsored Trolls and Their Influence on the Web" (WWW '19: Companion Proceedings of The 2019 World Wide Web Conference, March 4, 2019), https://arxiv.org/pdf/1801.09288.pdf.

72. Adam Goldman, Julian E. Barnes, Maggie Haberman, and Nicholas Fandos, "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump," *The New York Times*, February 20, 2020, https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html.

73. "IRA in Ghana: Double Deceit," Graphika, March 2020, https://graphika.com/uploads/Graphika_Report_IRA_in_Ghana_Double_Deceit.pdf.

74. Tony Romm and Craig Timberg, "Facebook, Twitter suspend Russian-linked operation targeting African Americans on social media," *The Washington Post*, March 12, 2020, https://www.washingtonpost.com/technology/2020/03/12/facebook-russia-african-americans-2020/.

75. "Case Studies – Collated – NOV 2019," The Computational Propaganda Project, November 2019, 92, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/Case-Studies-Collated-NOV-2019-1.pdf.

76. King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument."

77. Jessica Chen Weiss, "Understanding and Rolling Back Digital Authoritarianism," War on the Rocks, February 17, 2020, https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/.

78. Allie Funk, "A Grim Reality for Internet Freedom in Asia," Freedom House, November 7, 2018, https://freedomhouse.org/blog/grim-reality-internet-freedom-asia.

79. Lee and Sullivan, "People's Republic of the United Nations."

80. "Symposium on China-Kenya Cooperation and Development of Digital Economy successfully held in Kenya," China Federation of Internet Societies, December 16, 2019, http://www.en.cfis.cn/2019-12/16/c_1125352708.htm.; "CFIS held the China-Brazil Internet Governance Seminar successfully," China Federation of Internet Societies, January 10, 2020, http://www.en.cfis.cn/2019-12/16/c_1125352587.htm.; "The China-Cuba Internet Development Forum was successfully held," China Federation of Internet Societies, January 10, 2020, http://www.en.cfis.cn/2020-01/10/c_1125446738.htm.; "CFIS held the China-Brazil Internet Governance Seminar successfully,"

China Federation of Internet Societies, January 10, 2020, http://www.en.cfis.cn/2019-12/16/c_1125352587.htm.

81. Admin A, "China Involved in ESAT Jamming," Addis Neger Online, June 22, 2010, https://web.archive.org/web/20100703155601/http://addisnegeronline.com/2010/06/china-involved-in-esat-jamming; Christof Hartmann and Nele Noesselt, eds., *China's New Role in African Politics* (New York: Routledge, 2019), https://books.google.com/books?id=ch24DwAAQBAJ; and "Ethiopian Satellite Television (ESAT) accuses China of complicity in jamming signals," ECADF, June 15, 2011, https://ecadforum.com/2011/06/15/ethiopian-satellite-television-esat-accuses-china-of-complicity-in-jamming-signals/.

82. Tim Lister, Sebastian Shukla, and Nima Elbagir, "Fake news and public executions: Documents show a Russian company's plan for quelling protests in Sudan," CNN, April 25, 2019, https://www.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html.

83. Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *The New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.ht.

84. A. Ananthalakshmi, "RPT-Ahead of Malaysian Polls, bots flood Twitter with pro-government messages," Reuters, April 20, 2018, https://www.reuters.com/article/malaysia-election-socialmedia/rpt-ahead-of-malaysian-polls-bots-flood-twitter-with-pro-government-messages-idUSL3N1RY034.

85. Ryan Broderick and Íñigo Arredondo, "Meet the 29-Year-Old Trying to Become The King Of Mexican Fake News," Buzzfeed News, June 28, 2018, https://www.buzzfeednews.com/article/ryanhatesthis/meet-the-29-year-old-trying-to-become-the-king-of-mexican.

86. Isaac Stone Fish, "How China gets American companies to parrot its propaganda," *The Washington Post*, October 11, 2019, https://www.washingtonpost.com/outlook/how-china-gets-american-companies-to-parrot-its-propaganda/2019/10/11/512f7b8c-eb73-11e9-85c0-85a098e47b37_story.html.

87. Laura Wagner, "Internal Memo: ESPN Forbids Discussion of Chinese Politics When Discussing Daryl Morey's Tweet About Chinese Politics," Deadspin, October 8, 2019, https://deadspin.com/internal-memo-espn-forbids-discussion-of-chinese-polit-1838881032.

88. Krejsa, "Under Pressure: The Growing Reach of Chinese Influence Campaigns in Democratic Societies."

89. Leskin, "Here are all the major US tech companies blocked behind China's 'Great Firewall.'"

90. Sam Schechner and Gregory White, "U.S. Social-Media Giants Are Resisting Russia Censors," *The Wall Street Journal*, December 26, 2014, https://www.wsj.com/articles/u-s-tech-firms-face-showdown-with-russian-censors-1419620113.

91. "Instagram submits to Russia censor's demands," BBC, February 15, 2018, https://www.bbc.com/news/technology-43070555.

92. "Russian Watchdog Fines Google Over Violations, Warns Twitter and Facebook," TheMoscowTimes.com, December 11, 2018, https://www.themoscowtimes.com/2018/12/11/russian-watchdog-fines-google-over-violations-warns-twitter-facebook-a63781.

93. Sergei Blagov, "Facebook, Twitter Fined in Russia Over Data-Storage Practices," Bloomberg Law, February 13, 2020, https://news.bloomberglaw.com/privacy-and-data-security/facebook-twitter-fined-in-russia-over-data-storage-practices; and Marc Bennetts, "Facebook and Twitter could be blocked in Russia in data storage row," *The Guardian*, April 17, 2019, https://www.theguardian.com/world/2019/apr/17/facebook-and-twitter-face-russian-sanctions-in-data-storage-row.; Blagov, "Facebook, Twitter Fined in Russia Over Data-Storage Practices"; and Bennetts, "Facebook and Twitter could be blocked in Russia in data storage row."

94. Andrea Kendall-Taylor and David Shullman, "How Russia and China Undermine Democracy," *Foreign Affairs* (October 2, 2018), https://www.foreignaffairs.com/articles/china/2018-10-02/how-russia-and-china-undermine-democracy.

95. This insight draws from commentary made by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security.

96. Grove, "Russia Gives China a Leg Up in Foreign Broadcasting."

97. Ajit Singh and Max Blumenthal, "China detaining millions of Uyghurs? Serious problems with claims by US-backed NGO and far-right researcher 'led by God' against Beijing," The Gray Zone, December 21, 2019, https://thegrayzone.com/2019/12/21/china-detaining-millions-uyghurs-problems-claims-us-ngo-researcher/.

98. Hua Chunying (spokespersonCHN), "It seems that some US officials enjoy smearing China around the clock & around the world. What they say about Xinjiang is the LIE of the CENTURY. LYING and CHEATING won't make you nobler and greater. Why not come to Xinjiang and see with your own eyes." March 11, 2020, 11:07 p.m., Twitter, https://twitter.com/SpokespersonCHN/status/1237953397644390400.

99. "Moscow calls for joint cooperation with Beijing against U.S. interference."

100. "Hong Kong unmasked: The real reasons & instigators behind anti-Beijing riots," RT, December 1, 2019, https://www.rt.com/news/474756-hong-kong-protests-china-us/.

101. Fatima Tlis, "Russian 'Troll Farm' Posts Ersatz Report on Hong Kong Thanksgiving Rally," Polygraph.info, December 3, 2019, https://www.polygraph.info/a/fact-check-russian-troll-farm-hong-kong-usa/30305973.html.

102. Matina Stevis-Gridneff, "Blocked in U.S., Huawei Touts 'Shared Values' to Compete in Europe," *The New York Times*, December 27, 2019, https://www.nytimes.com/2019/12/27/world/europe/huawei-EU-5G-Europe.html.

103. Stevis-Gridneff, "Blocked in U.S., Huawei Touts 'Shared Values' to Compete in Europe."

104. Nathan Hodge, "Putin and Xi show a unified front against Trump in St. Petersburg," CNN, June 8, 2019, https://edition.cnn.com/2019/06/08/europe/putin-xi-st-petersburg-intl/index.html.

105. William J. Broad, "Your 5G Phone Won't Hurt You. But Russia Wants You To Think Otherwise," *The New York Times*, May 12, 2019, https://www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html.

106. "The Alliance for Securing Democracy Launches Hamilton 2.0 Dashboard," The German Marshall Fund of the United States, September 4, 2019, http://www.gmfus.org/press-releases/alliance-securing-democracy-launches-hamilton-20-dashboard.

107. Zak Doffman, "Huawei Soars In Russia As Putin Engages In New 'Technological War,'" *Forbes* (November 3, 2019), https://www.forbes.com/sites/zakdoffman/2019/11/03/huawei-soars-in-russia-as-putin-engages-in-new-technological-war/#738ed606765c. This section overall contains insights drawn from commentary made by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security.

108. European External Action Service Special Report, "Disinformation on the Coronavirus—Short Assessment of the Information Environment," March 19, 2020, https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/.

109. "Feast in time of plague? Trump official says China coronavirus is good for US economy," RT, January 31, 2020, https://www.rt.com/business/479668-coronavirus-could-boost-us-jobs/; and "Pompeo adds insult to injury by dangling coronavirus 'help' in front of sanctions-stricken Iran," RT, February 28, 2020, https://www.rt.com/news/481947-iran-pompeo-coronavirus-insult-sanctions/.

110. Tony Romm, "Millions of tweets peddled conspiracy theories about coronavirus in other countries, an unpublished U.S. report says," *The Washington Post*, February 29, 2020, https://www.washingtonpost.com/technology/2020/02/29/twitter-coronavirus-misinformation-state-department/.

111. Lijian Zhao (zlj517), "This article is very much important to each and every one of us. Please read and retweet it. COVID-19: Further Evidence that the Virus Originated in the US." March 12, 2020, 8:02 p.m. Twitter, https://twitter.com/zlj517/status/1238269193427906560; and Romm, "Millions of tweets peddled conspiracy theories about coronavirus in other countries, an unpublished U.S. report says."

112. Larry Romanoff, "COVID-19: Further Evidence that the Virus Originated in the US," Global Research, March 11, 2020, https://www.globalresearch.ca/COVID-19-further-evidence-virus-originated-us/5706078.

113. 安杰罗，"为什么武汉这场瘟疫，必须得靠解放军 [Why does the plague in Wuhan depend on the PLA]? Huarenjie.com, January 31, 2020, https://www.huarenjie.com/thread-8005070-1-1.html.

114. See, for example, "Virus may have circulated in Italy before outbreak in China," China Global TV Network (CGTN), March 22, 2020, https://www.youtube.com/watch?v=KELvvknOKSw&utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioschina&stream=china; and Bethany Allen-Ebrahimian, "Beijing's coronavirus propaganda blitz goes global," Axios, March 11, 2020, https://www.axios.com/beijings-coronavirus-propaganda-blitz-goes-global-f2bc610c-e83f-4890-9ff8-f49521ad6a14.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioschina&stream=china.

115. Kristine Lee and Ashley Feng, "How China set forth the global coronavirus crisis into motion," The Hill, March 12, 2020, https://thehill.com/opinion/international/487357-how-china-set-forth-the-global-coronavirus-crisis-into-motion.; Hua Chunying (SpokespersonCHN), "Amid the Chinese anthem playing out in Rome, Italians chanted 'Grazie, Cina!'. In this community with a shared future, we share weal and woe together." March 14, 2020, 11:09 p.m. Twitter, https://twitter.com/SpokespersonCHN/status/1239041044580188162; and Embaixada da China em Angola (ChinaEmbAngola), "Estudantes angolanos no Instituto Confucius solidarizam-se com a China.#COVID19." March 16, 2020, 5:38 a.m. Twitter, https://twitter.com/ChinaEmbAngola/status/1239501294911586304.

116. Francesco Bechis and Gabriele Carrer, "How China unleashed Twitter bots to spread COVID-19 propaganda in Italy," Formiche, March 23, 2020, https://formiche.net/2020/03/china-unleashed-twitter-bots-covid19-propaganda-italy/.

117. "Data Intelligence Comunicazione Cinese in Italia," Formiche by Alkemy SpA's R&D Lab, March 23, 2020, https://formiche.net/files/2017/07/Social-Data-Intelligence-Comunicazione-cinese-ricerca-per-Formiche-1.pdf.

118. "Full Text: International Strategy of Cooperation on Cyberspace," Xinhua, March 1, 2017, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_3.htm.

119. "Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance," Global Commission on Internet Governance, January 17, 2017, https://www.cigionline.org/publications/who-runs-internet-global-multi-stakeholder-model-internet-governance.

120. "6th World Internet Conference opens in China's Zhejiang," Xinhua, October 20, 2019, http://www.xinhuanet.com/english/2019-10/20/c_138487994.htm.

121. Justin Sherman and Mark Raymond, "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom," *The Washington Post*, December 4, 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/.

122. Joe Uchill, "Russia and China get a big win on internet 'sovereignty,'" Axios, November 21, 2019, https://www.axios.com/russia-china-united-nations-internet-sovereignty-3b4c14d0-a875-43a2-85cf-21497723c2ab.html.

123. "Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online," Association for Progressive Communications, November 2019, https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.

124. Sherman and Raymond, "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom."

125. Josh Gold, "The First Ever Global Meeting on Cyber Norms Holds Promise, But Broader Challenges Remain," Council on Foreign Relations' Net Politics blog on CFR.org, September 30, 2019, https://www.cfr.org/blog/first-global-meeting-cyber-norms.

126. This insight reflects commentary made by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security.

127. "5th Russia-China Media Forum to Be Held at EEF 2019," Roscongress, August 13, 2019, https://roscongress.org/en/news/5th-russiachina-media-forum-to-be-held-at-eef-2019/.

128. Shi Jing, "China-Russia digital media cooperation forum boots up in Wuxi," *China Daily*, November 15, 2019, https://www.chinadaily.com.cn/a/201911/15/WS5dce4766a310cf3e35577aa0_1.html.

129. Samuel Bendett and Elsa B. Kania, "A new Sino-Russian high-tech partnership," Policy brief Report No. 22/2019 (Australian Strategic Policy Institute, October 2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/A%20new%20Sino-Russian%20high-tech%20partnership_0.pdf?xAs9Tv5F.GwoKPiV9QpQ4H8uCOet6Lvh.

130. Sarah Cook, "Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017" (Freedom House, January 2020), https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone#footnote2_w7knna3.

131. "The Alliance for Securing Democracy Launches Hamilton 2.0 Dashboard."

132. Khandaker, "The WeChat factor."

133. "Sputnik Signs Cooperation Agreements With China's Xinhua, Guangdong Agencies," Sputnik, April 7, 2017, https://sputniknews.com/agency_news/201707041055212186-sputnik-agreement-xinhua-cooperation/.

134. This insight reflects commentary made by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security; see, for example, Colum Murphy and Zheping Huang, "China's Red-Hot Face-Swapping App Provokes Privacy Concerns," Bloomberg, September 1, 2019, https://www.bloomberg.com/news/articles/2019-09-02/china-s-red-hot-face-swapping-app-provokes-privacy-concern; Peter Suciu, "TikTok's Deepfakes Just The Latest Security Issue For The Video Sharing App," *Forbes* (January 7, 2020), https://www.forbes.com/sites/petersuciu/2020/01/07/tiktoks-deepfakes-just-the-latest-security-issue-for-the-video-sharing-app/#570476e870a2.

135. Hannah Denham and Drew Harwell, "Panic over Russian company's FaceApp is a sign of new distrust of the Internet," *The Washington Post*, July 18, 2019, https://www.washingtonpost.com/technology/2019/07/18/heres-what-we-know-about-russian-company-behind-faceapp/.

136. Jill Dougherty and Molly Jay, "Russia Tries to Get Smart About Artificial Intelligence," *The Wilson Quarterly* (Spring 2018), https://www.wilsonquarterly.com/quarterly/living-with-artificial-intelligence/russia-tries-to-get-smart-about-artificial-intelligence/.

137. Li, "Russia is Beijing's best ally in the disinformation war against Hong Kong"; and DFRLab, "Telegram channels used to doxx and report Hong Kong protesters to Chinese authorities," Medium, September 25, 2019, https://medium.com/dfrlab/telegram-channels-used-to-doxx-and-report-hong-kong-protesters-to-chinese-authorities-91bed151f345.

138. "Sino-Russian media cooperation and exchange enters a new era," Xinhua, September 3, 2019, http://www.xinhuanet.com/world/2019-09/03/c_1124957041.htm.

139. He Huifeng, "In a remote corner of China, Beijing is trying to export its model by training foreign officials the Chinese way," *South China Morning Post*, July 14, 2018, https://www.scmp.com/news/china/economy/article/2155203/remote-corner-china-beijing-trying-export-its-model-training.

140. This insight reflects commentary made by Laura Rosenberger at a November 20, 2019, workshop at the Center for a New American Security.

141. A leading example of high-quality analysis is the Alliance for Securing Democracy at the German Marshall Fund of the United States: https://securingdemocracy.gmfus.org/. Examples of university scholarship include Oxford University's Computational Propaganda Project and the University of Washington's Center for an Informed Public: https://comprop.oii.ox.ac.uk/, https://www.cip.uw.edu/.

142. Nicola Smith, "Schoolkids in Taiwan Will Now Be Taught How to Identify Fake News," *Time* (April 7, 2017), https://time.com/4730440/taiwan-fake-news-education/; and Emma Charlton, "How Finland is fighting fake news – in the classroom," World Economic Forum, May 21, 2019, https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/.

143. For example, see "Our K-12 Digital Citizenship Curriculum," Education Week, https://www.edweek.org/media/k-12-digital-citizenship-curriculum.pdf; and Sarah Perez, "Google's new media literacy program teaches kids how to spot disinformation and fake news," Tech Crunch, June 24, 2019, https://techcrunch.com/2019/06/24/googles-new-media-literacy-program-teaches-kids-how-to-spot-disinformation-and-fake-news/.

144. Niraj Chokshi, "Older People Shared Fake News on Facebook More Than Others in 2016 Race, Study Says," *The New York Times*, January 10, 2019, https://www.nytimes.com/2019/01/10/us/politics/facebook-fake-news-2016-election.html.

145. The authors are indebted to Laura Rosenberger for feedback on an initial draft of this report that substantially shaped the final version of this recommendation.

146. Laura Rosenberger and Zack Cooper, "Why it's time for the U.S. to start pushing back against Chinese information operations," *The Washington Post*, September 9, 2019, https://www.washingtonpost.com/opinions/2019/09/09/why-its-time-us-start-pushing-back-against-chinese-information-operations/; and Kara Frederick, "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight" (Center for a New American Security, June 3, 2019), https://www.cnas.org/publications/reports/the-new-war-of-ideas.

147. A similar recommendation is made by Adrian Shahbaz in "How Technology Platforms Should Deal with Hostile State-Owned Propaganda Outlets," Freedom House, press release, August 20, 2019, https://freedomhouse.org/article/how-technology-platforms-should-deal-hostile-state-owned-propaganda-outlets.

148. "G7 Rapid Response Mechanism Backgrounder," Government of Canada, January 30, 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html; and Matt Apuzzo, "Europe Built a System to Fight Russian Meddling. It's Struggling," *The New York Times*, July 6, 2019, https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html.

149. Noah Barkin, "Exclusive: Five Eyes intelligence alliance builds coalition to counter China," Reuters, October 12, 2018, https://www.reuters.com/article/us-china-fiveeyes/exclusive-five-eyes-intelligence-alliance-builds-coalition-to-counter-china-idUSKCN1MM0GH.

150. "Who we are: Governing Council," Community of Democracies, https://community-democracies.org/?page_id=58.

151. Joe Uchill, "More than 50 nations, but not U.S., sign onto cybersecurity pact," Axios, November 12, 2018, https://www.axios.com/cybersecurity-paris-call-for-trust-france-21e434df-8a59-48bc-8cde-cd1c1f43dfd0.html.

152. This last recommendation was also put forward in Ely Ratner, Daniel Kliman, Susanna Blume, Rush Doshi, Chris Dougherty, Richard Fontaine, Peter Harrell, Martijn Rasser, Elizabeth Rosenberg, Eric Sayers, Daleep Singh, Paul Scharre, and Loren DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific" (Center for a New American Security, December 2019), 46, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-NDAA-final-6.pdf?mtime=20200116130752.

153. For a comprehensive survey of Beijing's approach to ethnic Chinese living overseas, see Timothy Heath, "Beijing's Influence Operations Target Chinese Diaspora," War on the Rocks, March 1, 2018, https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora/.

154. Jan Lopatka, "Radio Free Europe launches new Russian-language TV channel," Reuters, February 7, 2017, https://www.reuters.com/article/usa-russia-rfe/radio-free-europe-launches-new-russian-language-tv-channel-idUSL5N1FS54Q; and "Jobs and Internships: Digital Content Producer, Global Mandarin," Radio Free Asia, December 9, 2019, https://www.rfa.org/about/jobs-and-internships/digital-content-producer-global-mandarin-09122019155250.html.

155. An example of Beijing's support for its media companies in the developing world is StarTimes in Africa. Jenni Marsh, "How China is slowly expanding its power in Africa, one TV set at a time," CNN Business, July 24, 2019, https://www.cnn.com/2019/07/23/business/star-times-china-africa-kenya-intl/index.html; and Cook, "Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017."

156. An earlier variant of this recommendation was first put forward in Lee and Barbesino, "Challenging China's Bid for App Dominance."

157. A variant of this recommendation was initially advanced by CNAS Fellow Kara Frederick; see Frederick, "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight."

158. U.S. Cyber Command is reportedly developing this option for use against Russia in the event of election interference in 2020. Ellen Nakashima, "U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election," *The Washington Post*, December 25, 2019, https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html.

159. Targeting a wide range of actors with sanctions is the best way to deter the largest number from future undesirable behavior. Elizabeth Rosenberg and Jordan Tama, "Strengthening the Economic Arsenal" (Center for a New American Security, December 2019), https://www.cnas.org/publications/reports/strengthening-the-economic-arsenal.

160. A similar recommendation is made by Fly, Rosenberger, and Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies."

161. Ratner, Kliman, et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific."

162. For a related argument, see Kurt M. Campbell and Rush Doshi, "The Coronavirus Could Reshape Global Order," *Foreign Affairs* (March 18, 2020), https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org


Center for a
New American
Security