The Washington Quarterly

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rwaq20

How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks

Jessica Brandt

To cite this article: Jessica Brandt (2021) How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks, The Washington Quarterly, 44:3, 127-154, DOI: 10.1080/0163660X.2021.1970902

To link to this article: https://doi.org/10.1080/0163660X.2021.1970902

Published online: 22 Sep 2021.

Jessica Brandt

How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks

Democracies are engaged in a broad, persistent asymmetric competition with authoritarian challengers who seek to reshape the global order to suit their interests. The competition is playing out across multiple intersecting domains, and the information space is a critical theater.[1] In this competition, Russia and China intentionally choose tools that give them the upper hand.

In the political domain, Russia and China take advantage of permissive influence regimes, covertly funneling millions of dollars to political parties and civil society groups to sway policy decisions.[2] They exploit democracies' visible domestic challenges—from inequality to polarization—in the service of deepening social divides. And they conduct cyberattacks against legislatures, businesses, media organizations, and other entities to cripple a target society or retaliate against those that would hold them accountable. In the economic domain, Russia deploys corruption as an instrument of national strategy, transforming the grift that was once simply a routine feature of its own society into a weapon for subverting democratic ones.[3] Both regimes cultivate economic dependencies, make coercive investments, and deploy unfair trade practices as leverage.[4] In the technology domain, China is investing significant resources into attaining an edge in global markets. As it does so, it is shaping the standards for how new technologies will be developed and the norms that will govern how they will be used for decades to come, with potentially significant consequences for the rights to privacy and expression of individuals worldwide.[5]

Jessica Brandt is Policy Director of the AI and Emerging Technology Initiative at the Brookings Institution and a Fellow in its Foreign Policy Program. She can be followed on Twitter @jessbrandt.

The Washington Quarterly • 44:3 pp. 127–154
https://doi.org/10.1080/0163660X.2021.1970902

All of this activity is consequential, yet it is in the information domain that Moscow and Beijing have identified and leveraged some of the sharpest asymmetries. Both deliberately spread or amplify information that is false or misleading. Russia frequently engages in deceptive practices such as misrepresenting the origin of content or its intent.[6] Both invest large sums in propaganda networks that proliferate their preferred, distorted narratives. In order to draw a false equivalence with their own illiberal systems, both deploy "whataboutism" to paint the United States as hypocritical, particularly on issues of race. Both have spread multiple, at times conflicting, conspiracy theories to deflect criticism of their misdeeds and erode the idea that there is such a thing as objective truth. Moscow deploys a network of proxy influencers to churn up anti-western sentiment, while Beijing has worked to control digital distribution channels in the Chinese-speaking world and co-opt independent media abroad.[7] For Putin and Xi, the goal of these pursuits is to maintain a grip on power at home and weaken democratic competitors abroad.

Putin and Xi seek to maintain power at home and weaken democratic competitors abroad

Russia and China pursue this approach because even as open information spaces confer important strategic advantages to democracies over the long run, they create vulnerabilities for them in the short term.[8] Free societies—where academics, journalists, and activists are connected to counterparts around the world—can be easily disrupted using low-cost, deniable tools. And while democracy depends on the idea that the truth is knowable and that citizens can discern it and harness it to govern themselves, authoritarians have no such need for a healthy information space to thrive.[9] That means they can pollute the information commons without great concern for eroding the strength of their own institutions. In fact, quite the opposite: autocrats are vulnerable to the free flow of information that might expose their failures or false promises, and benefit from widespread public skepticism that truth exists at all.[10]

To date, the United States and other liberal democracies have been slow to appreciate the nature of the contest with authoritarian regimes and to develop a proactive strategy to push back. This is especially the case in the information domain, which is perhaps the most consequential terrain over which rival states will compete in the century to come.[11] This latency is partially driven by the challenge of developing a coherent threat assessment when so much of the relevant activity is occurring on millions of smart phones instead of conventional battlefields. But it is primarily a result of the hands-off approach democracies have traditionally taken to dealing with information—and for good reason, given that they risk contravening Kennan's admonition not to become like those

whom they are competing against.[12] Those constraints will make it hard for democratic societies to contend with Russia and China's online information manipulation activities, but they need not forestall success.[13]

The United States and other liberal democracies need a strategy to counter Russia and China's online information manipulation activities—one that is informed by a detailed understanding of the challenge. This article aims to contribute to that understanding by highlighting the contours of Russia and China's information strategies, noting where their goals differ and converge, and by presenting a catalogue of their tradecraft, which can edify policymakers across public and private sectors. It concludes by identifying recent changes in their strategy, forecasting the trajectory of this activity, and offering ideas for how democratic societies can rise to the challenge.

Are Russia and China's Goals the Same?

Russia and China operate from different strategic positions and trajectories, on distinct time horizons, with disparate tolerance for risk, and toward divergent long-term goals. By many measures, Russia is a declining power. Russia's GDP reached only about 8 percent of the United States' in 2019,[14] and its economy contracted by more than 3 percent last year, driven by the coronavirus pandemic and the related fall in global energy demand.[15]

To compensate for Russia's relative weakness, Putin seeks to disrupt the alliances, institutions, and domestic politics of competitor states, and to do so in the near term. Unlike Xi, Putin has little interest in ensuring a stable global order. As analysts Laura Rosenberger and John Garnaut have observed, Putin instead advances "a more limited objective of weakening the current order to gain relative strength—his only means to Make Russia Great Again—and maintain his own authority."[16] With little to lose and much to gain from public awareness of its activities, the Kremlin is not particularly sensitive to attribution. As a result, Russia's interference activities generally—and its information manipulation activities specifically—tend to be destructive, aimed at promoting disarray, with little concern for the repercussions. The Kremlin does not seek to attract audiences to Russia or promote a particular worldview, but rather to promote the idea that there is no such thing as objective truth.[17] It can be a brutal pursuit. While both Putin and Xi endeavor to suppress criticism of their own regimes and preserve their grip on power, only Putin has shown himself willing to execute political opponents abroad for that purpose.[18]

Unlike during the Soviet era, the Kremlin's interference activity tends to be carried out in a decentralized manner. It practices what professor Mark Galeotti has called "authoritarian entrepreneurialism," whereby Putin and his inner circle

frame their objectives in broad terms, and numerous proxies, from diplomats to hackers, endeavor to fulfil them.[19] As Galeotti has observed, this activity is "voluntarist and dispersed"—there appears to be some effort to coordinate particular operations, but often only after action has been taken by an individual agent.[20] Russia's troll farms, like its proxy websites, are linked to the Kremlin through a network of non-transparent personal and financial ties.[21] Nevertheless, multiple elements of the state—from its intelligence services to its propaganda outlets—have a hand in interference endeavors.[22] And there is mounting evidence that the Kremlin's reliance on its intelligence services to carry out deceptive campaigns is growing as Moscow works to circumvent the platform and other detection mechanisms that were put in place after its 2016 operation.[23]

China, by contrast, is a rising power that has been steadily growing its economic, technological, and military strength over decades. Partly as a result of the shockwaves the coronavirus pandemic has sent rippling through global markets, it is projected to become the world's largest economy within the decade—five years sooner than previously anticipated.[24] Ten percent of global patent activity takes place within its borders.[25] And its defense spending jumped tenfold since the mid-1990s, from less than 3 percent of the global total to more than 14 percent by 2019.[26]

Unlike Russia, China is pursuing a subtle, long-term strategy to reshape the international system

In light of these trends, China prefers a stable international order, though one that is more conducive to its interests than the current US-led architecture. Unlike Russia, it is pursuing a subtle, long-term strategy to reshape the international system.[27] Beijing hopes, as now-Director for China at the National Security Council Liza Tobin put it in 2018, that its "global network of partnerships centered on China would replace the US system of treaty alliances, the international community would regard Beijing's authoritarian governance model as a superior alternative to Western electoral democracy, and the world would credit the Communist Party of China for developing a new path to peace, prosperity, and modernity that other countries can follow."[28]

This strategy frequently entails patiently cultivating relationships with elite intermediaries abroad that can be exploited opportunistically to favorably shape perceptions of China and wielding economic leverage for the same purpose.[29] As a rising power with much to lose from having its engagement in information operations exposed, China has traditionally been more sensitive to attribution than its Russian counterparts, although there is some evidence that Beijing is more comfortable with an openly assertive information strategy in

the context of the coronavirus pandemic. Driven by fear that China could be seen as responsible for a disaster that has wrought such an immense human and economic toll, Beijing has begun leveraging an army of Twitter assets that it began amassing in 2019 amid accelerating Hong Kong protests.[30]

China's activities are carried out by the United Front system, which China analyst Alex Joske describes as "a network of party and state agencies responsible for influencing groups outside the party, particularly those claiming to represent civil society. It manages and expands the United Front, a coalition of entities working towards the [Chinese Communist Party]'s goals."[31] As researcher Matt Schrader has detailed, Chinese Communist Party (CCP) organs such as the Ministry of Propaganda, the People's Liberation Army (PLA), and the United Front Work Department each play a role.[32]

Despite these important distinctions, Russia's and China's information strategies share three immediate objectives. As Rosenberger and Garnaut observed, both have an interest in undermining the legitimacy of liberal democratic systems and governments, as a means of shoring up their own illiberal ones. Both aim to stifle criticism from foreign individuals or governments and prevent them from coordinating to counter their interests. And both seek to weaken global alliances, partnerships, and institutions that could constrain their activities.[33]

There is little evidence of explicit coordination between Moscow and Beijing on strategies or tactics aside from limited, largely symbolic agreements to distribute one another's content through state media.[34] That is not surprising, given that neither party requires formal collaboration to achieve its aims. Beijing in particular does not need to secure official cooperation with the Kremlin in order to emulate elements of its information strategy, as plenty of other far less sophisticated actors have done, nor to amplify anti-Western narratives promoted by the Kremlin's network of proxy influencers that are conducive to its own interests. Even if they are not coordinated and do not share long-term aims, Russia's and China's activities in the information domain are having a compounding, corrosive effect on the information environment—closing space for public discourse on which democracy depends.

There is little evidence of explicit coordination between Moscow and Beijing

Because many elements of Beijing's and Moscow's online information manipulation activity are not transparent—and because much of it is connected to offline pursuits—developing a coherent threat picture has proven challenging to democratic governments. But thanks to the work of journalists, academics, and civil society researchers, rich investigative accounts are increasingly

available in the public domain.[35] In many cases, these have been catalyzed by more frequent, detailed warnings from intelligence agencies, which alongside bipartisan Senate investigations have contributed to a substantial body of relevant literature.[36] This is fortunate, since understanding tradecraft is important for mounting an effective response.

Russia's Maturing Playbook: How It Is Evolving

To carry out its objectives in the information domain, the Russian government and its proxies use a suite of evolving techniques to conduct deceptive campaigns. By now, it is well documented that Russia and its proxies seek to drive polarization up and trust in institutions down by amplifying the most divisive content that already exists in a target society to make it appear more salient. The strategic leak of hacked, at times manipulated, materials is an intermittent element of this strategy. This section aims to highlight some of the most important, recent techniques of relevance to policymakers, drawing on what is publicly known about Russia's online information manipulation activities since 2016.[37]

Co-Opting Authentic Domestic Voices and Institutions

The Kremlin and its proxies work to co-opt legitimate domestic voices within target societies, particularly those of journalists and activists, in order to disguise an operation as authentic advocacy. They accomplish this through a range of techniques, among them co-locating trolls within a target population. More than 30 Russian agents were working inside Madagascar ahead of that country's 2018 presidential election, for example—publishing their own newspaper in the local language and hiring local students to write for it, paying local youth to attend rallies and hiring journalists to cover them, and recruiting a spoiler candidate to run in an effort to split the opposition vote.[38] In Cameroon, Central African Republic, Democratic Republic of the Congo, Libya, Mozambique, and Sudan, Russian actors worked with local citizens to create authentic-seeming accounts that posted content promoting Russian policies in Africa and criticizing those of France and the United States.[39]

Russian agents have also rented the social media accounts of local users with the goal of using the accounts to publish political ads or plant articles, including in Ukraine ahead of its 2019 presidential election.[40] And in multiple countries in what Russia deems its "near abroad," including Ukraine and Georgia, Russian military operatives have used false personas to entrap local leaders in "interviews" with purported journalists on politically sensitive subjects, inviting their targets to make divisive comments in direct messages and then posting screenshots of their exchanges in order to inflict political damage.[41] In the United States,

Russian agents used a false persona to recruit a legitimate, self-described anti-fascist domestic activist to serve as the administrator of a Facebook group that organized numerous political protests ahead of the 2018 midterm elections.[42] Ahead of the 2020 US presidential election, Russian agents hired freelance journalists to write political stories for an online publication secretly run by individuals linked to the Internet Research Agency (IRA).[43] And it used proxies linked to Russian intelligence to seed misleading narratives with prominent individuals, media organizations, and officials in the United States to facilitate the spread of those narratives across the broader information ecosystem, including offline.[44] This activity has increasingly also entailed mimicking or appropriating the identities of domestic nonprofits.[45]

Russia and its proxies co-opt authentic domestic voices and institutions for three reasons. The first is that it improves operational security—not primarily to prevent attribution, but to stop its activity from being thwarted from the start by platform detection mechanisms that have grown increasingly sophisticated. Where early IRA trolls were identified because their registration data, including IP addresses and phone numbers, were inconsistent with their stated locations, operations run by domestic actors have local IP addresses; they also take on the colloquialisms of the target society. Second, the approach implicates constitutional protections on free expression and triggers fraught political dynamics that complicate the response options available to platforms and governments. Ahead of the 2020 presidential election, social media platforms received substantial blowback for removing or reducing the distribution of an unsubstantiated *New York Post* article that contained a cache of files and emails supposedly taken from the laptop of the son of the Democratic presidential nominee. Although it remains unclear what role, if any, the Kremlin played in that episode, it is hard to imagine that Putin and his proxies were anything short of pleased by the partisan paroxysms that it triggered.[46] Third, a movement that is discovered to have been infiltrated by foreign operatives can be discredited, creating yet another opportunity to stoke domestic turmoil. In 2019, for example, authentic African American activists raised concern that their genuine advocacy had been disparaged as the work of bots, dampening its effectiveness by calling into question its credibility, in an episode that ultimately triggered recriminations within the movement itself.[47]

> Entrapping local leaders is more in keeping with Moscow's efforts than Beijing's

Beijing cultivates intermediaries in target societies, but this is generally a hallmark of its offline information manipulation activity where it frequently applies coercive economic leverage to suppress criticism (rather than to seed polarizing narratives, as Russia does). Entrapping local leaders and recruiting authentic

freelancers to produce polarizing commentary on political events are techniques aimed at driving up polarization, a goal more in keeping with Moscow's efforts to rend target societies from within, undermining trust and order altogether, rather than Beijing's efforts to fashion an international order more conducive to its way of doing business.

Conducting Perception Hacks

Another frequent tactic is the "perception hack," where a small or questionably effective network seeds the idea that it is larger or more potent than it really is. Since the exposure of its "sweeping and systematic" effort to undermine the 2016 US presidential election, the Kremlin and its proxies have used this tactic to make inflated claims about alleged manipulation, including through a false flag operation. Shortly before polls closed on the day of the 2018 US midterm elections, for example, a website that claimed to be run by the IRA professed to have conducted a successful, clandestine interference campaign. It published a list of fake Instagram accounts and a spreadsheet purporting to be advance results of every Senate race, while affiliated individuals sent taunting messages to reporters in order to elicit coverage.[48] The operation failed to gain serious attention, thanks to wary journalists, but it demonstrated that, more than swaying the outcome of an election, the Kremlin is interested in discrediting elections entirely. More recently, the Kremlin and its proxies have seized opportunities to promote homegrown election manipulation conspiracy theories. In the aftermath of the 2020 Iowa Caucus debacle, for example—when an application malfunctioned, causing lengthy delays in the reporting of results—Russian state media and diplomatic accounts on Twitter amplified false claims that the election had been rigged by Democratic party elites and the "corporate media" as well as conspiracy theories alleging murky ties between various candidates and the company that created the application. Throughout 2020, Russian actors spread false or overblown claims about purported compromises of voting systems to undermine public confidence in the legitimacy of the democratic outcome.[49]

By taking a perception hacking approach, Moscow lowers the threshold for a successful operation. It does not need to evade platform detection capabilities, which have been steadily increasing since 2016, or perpetuate a vast operation to rend a target society from within. All it needs to do is create the impression that it might have interfered, which can alone be as damaging. A perception hacking approach also complicates efforts to unmask interference. If officials share too little information, they might undermine resilience by leaving the public uninformed; worse, they risk politicized leaks of misleading information. On the other hand, if officials share too much, they risk perpetuating the very concern that they seek to allay—that an election has been compromised.[50] For

this reason, perception hacks make it more difficult for democratic societies to build resilience to foreign interference threats.

Beijing has to date not engaged in the sort of election manipulation that provides the foundation for a perception hack. The US Intelligence Community assessed that China considered but did not deploy influence efforts targeted at the 2020 presidential election, because it did not want to risk getting caught meddling.[51] Fundamentally, perception hacking is about inflating one's own culpability for destructive activity. It is a strategy that is in keeping with Russia's risk-acceptant approach to interference, but not with China's more cautious one.

Exploiting the Full Information Ecosystem

Just as they might with illicit funds, the Russian government and its proxies launder information—placing, layering, and integrating it in ways that obscure its true origin—in order to apply a veneer of legitimacy.[52] Moscow uses quasi-transparent Russian government-supported media properties—including viral news video channels that are popular with young audiences on YouTube—to target young, left-leaning, Western audiences with Russia's propaganda narratives in the form of slick, "meme-able satire" under the guise of independent journalism.[53]

A network of proxy websites disseminates these narratives. The content that they produce and amplify—some of it published by Western fringe thinkers and conspiracists and much of it cross-posted to other websites in the network—enables disinformation to spread across other parts of the information ecosystem.[54] For example, the *Strategic Culture Foundation*, an online journal directed by Russia's Foreign Intelligence Service (SVR) and affiliated with the Russian Ministry of Foreign Affairs, is one of several propaganda outlets that regularly features Western authors for the purpose of obscuring its Russian origins. Others include *Global Research*, a Canadian website that has a "large roster of fringe authors and conspiracy theorists [that serve] as a talent pool for Russian and Chinese websites," according to an analysis published by the US Department of State. "Its publications also provide a Western voice that other elements of the ecosystem can leverage to their advantage."[55]

Moscow also exploits data voids, which occur when search engines have little content to return for a particular query, to shape narratives around sensitive topics. They do so by guiding users to search terms that they have coopted in order to surface content that they have curated.[56] Russian actors used this form of algorithmic manipulation in a 2017 campaign to smear the White Helmets, a volunteer humanitarian organization that documented a chemical weapons attack on Syrian civilians that UN war crimes investigators later

attributed to the Kremlin-supported regime. The campaign, which included gaming social media algorithms with a flood of content boosted by inauthentic accounts, aimed to falsely label the humanitarian group as terrorists in order to discredit and delegitimize their work.[57] For some time, RT and Sputnik content promoting this narrative was among the top search results for "White Helmets" on Google and YouTube.[58]

These operations exemplify Russia's efforts to engage multiple elements of the information environment to surface their propaganda narratives. And they are an illustration that sophisticated online information operations are not confined to users' news feeds—they spread across respected media outlets and sometimes, as the experience of 2020 showed, through domestic political figures.[59] This activity can be mutually reinforcing with broader efforts to amplify domestic conspiracy theories, including as part of perception hacking campaigns.[60] And it enables the Kremlin to create an echo chamber of support for its interests while depressing social trust.

By coopting authentic domestic voices and institutions, conducting perception hacking operations, and laundering narratives across the full information ecosystem, Russia furthers its objective of denigrating democratic governments and institutions and sowing seeds of political turmoil that rend democratic societies from within. In doing so, it seeks to distract liberal democratic governments, keeping them from coordinating with one another to play a forward-leaning role in world affairs that could run counter to the Kremlin's interests.

Beijing's Unique Tactics

To carry out China's goals in the information domain, Beijing has adopted some of Russia's playbook—including propagating multiple, conflicting conspiracies to cast doubt on official versions of politicized events and relying on a sprawling state media apparatus to promote narratives that denigrate Western democratic governments and institutions. But Beijing also deploys a number of tactics, tools, and techniques of its own, reflecting its interest in defending China's image as a responsible global superpower.

In the context of the coronavirus pandemic, though beginning shortly before it, China's official activity online has surged. The number of Beijing's government and diplomatic accounts on Twitter has grown nearly fivefold since the beginning of 2019. And the aggregate output of these accounts has grown too, from almost 5,000 tweets in January 2020 to roughly 15,000 tweets in January 2021.[61] All the while, the tone of China's official activity online has sharpened, as its "wolf warrior" diplomats—who take their name from a nationalistic Chinese film franchise—use Twitter to troll Beijing's rivals.[62] This section

highlights some of the most salient, recent, and unique tactics that Beijing is currently employing so that policymakers can learn from them in real time.[63]

Piggybacking on Other Strongmen's Propaganda Networks

In the absence of its own established network of proxy influencers, Beijing may be leveraging the propaganda networks of other autocrats—including Putin, but also Venezuela's Nicolás Maduro—to push anti-Western messaging that is broadly aligned with its geopolitical interests. These include narratives casting elements of US foreign policy as "ignor[ing] all moral limits" and painting the US Secretary of State as "a joke."[64] Over the last year and a half, Chinese diplomats retweeted Maduro more than any other non-Chinese account, although the overwhelming majority of this activity was driven by China's ambassador to Venezuela. During this same period, Russia's RT and Venezuela's TeleSur and VTV Canal 8 appear to have been among the 10 most frequently retweeted media outlets not operated by Beijing.[65]

> Since the pandemic, China's official online activity has surged.

Chinese diplomats also frequently amplify the alternative media channels, conspiracy thinkers, and pseudo-academics that are regularly featured on Russia's network of proxy websites.[66] For example, a recent piece that originally ran in anti-establishment alternative media outlet Grayzone, which attacked research on Xinjiang, was cited by China's state media and tweeted by "wolf warrior" diplomats on four continents.[67] Defined more by their reactionary opposition to Western foreign policy than any affinity to Beijing, these fellow travelers are nevertheless useful vectors to push Party-friendly narratives on Xinjiang, Hong Kong, and Taiwan.[68] Where China's amplification of Venezuelan content on Twitter is driven primarily by Beijing's ambassador to Venezuela, China's engagement with Russian content on the platform appears more evenly distributed among Beijing's corps of "wolf warriors."

Like Moscow, Beijing uses this approach in an effort to boost the reach and resonance of its messaging and to construct a façade of legitimacy around its preferred narratives, while obscuring its culpability for seeding them. This is especially the case for narratives that are confrontational or conspiratorial. Unlike Moscow, Beijing has thus far not appeared to develop a proxy network of its own. That may be because it is able to reap the benefits of the Kremlin's network without taking on risk itself. It may also be because it believes existing outlets, which have no links back to Beijing, lend the greatest legitimacy to its preferred narratives. Or it may simply be because Beijing's more assertive posture in the information space is new and evolving.

Manufacturing the Appearance of Popular Backing

Unlike Moscow, Beijing appears to rely on false personas to create the illusion of popular support for its messaging, particularly in circumstances when they are unable to develop substantial, organic traction on their own. That is, where Russia uses false personas to seed polarizing and divisive narratives or to entrap local journalists in an influence campaign, China uses them to make it look like an army of netizens agree with pro-China positions. On Twitter, China's diplomats regularly engage with accounts that bear multiple hallmarks of inauthenticity, including handles whose naming conventions suggest that they were computer generated or set up in haste (for example, a generic name followed by a sequence of numbers or an alphanumeric combination), creation dates within a short time span, and profile photos found elsewhere online.[69] Many of these accounts have been suspended by Twitter, including several that were, for a time, among those most frequently retweeted by Beijing's "wolf warriors."[70] More than 600 retweets of accounts that have subsequently been suspended were driven by just five of China's diplomats—Beijing's ambassador to Venezuela and its consuls general in Durban, Cape Town, Karachi, and Kolkata.[71]

Russian diplomats, by contrast, rarely engage with suspicious accounts. Not a single one of the 131 suspended accounts retweeted by Russian diplomats between April and October of last year, for example, was among the top 200 accounts they most frequently retweeted.[72] This approach likely reflects the difficulty Beijing faces in building an authentic audience on a platform that it bans within its borders.

Coopting Critical Conversations on Its Rights Record

Also unlike Moscow, China's diplomats have used hashtag campaigns and other tactics to crowd out conversations on its dismal human rights record with positive content. For example, #AmazingChina, #RealLifeXinjiang, #FactsSpeakLounder, and #GlamorChina are among the 20 most used hashtags in tweets from Beijing's diplomats covering the Xinjiang region, where the Chinese government carries out egregious human rights abuses against the Muslim Uighur population.[73] These accounts regularly share content featuring slick travel videos and purported "re-education" success stories.[74] Beijing has also rolled out a new, dedicated English-language state media account that proffers cheerful depictions of life in Xinjiang.

Whereas Moscow focuses on discrediting the West, Beijing seeks to soften how China is perceived

Where Moscow's information strategy appears to focus on discrediting the West, rather than attracting audiences to Russia, China is much more focused on softening

how it is perceived. Russia's state media almost never covers Russian domestic issues, culture, or politics. China's, by contrast, proactively promotes a positive image of the country and its governance model.[75]

Areas of Alignment: Where Russia and China's Playbook Overlap

Russia and China each deploy an evolving set of tactics and techniques to advance their geopolitical interests in the information domain. For Russia—which aims to stoke chaos and promote disorder in an effort to keep the political West distracted, divided, and unable to carry out an assertive, unified foreign policy that could be detrimental to the Kremlin's interests—that has entailed coopting authentic domestic voices and institutions, perpetuating perception hacks, and laundering narratives across large swaths of the information space. For China—which prefers a stable order more conducive to its interests and therefore seeks to promote its image as responsible global player and stifle criticism that would suggest otherwise—that has entailed piggybacking on the propaganda networks of other strongmen, manufacturing the appearance of popular support, and coopting conversations on its rights record.

Despite important differences in their long-term goals, Moscow and Beijing nevertheless share multiple near-term objectives, and as a result, deploy several of the same tactics including the use of "whataboutism," clickbait, conspiracy theories, and vast propaganda apparatuses to convey their preferred narratives.

Both Russia and China frequently rely on "whataboutism" to paint the United States as hypocritical, particularly on issues of race. Beijing's diplomats—who before the COVID-19 pandemic were typically reluctant to weigh in on social or political rights issues in other countries—used the #BlackLivesMatter, #GeorgeFloyd, and #IcantBreathe hashtags hundreds of times following the May 25, 2020 killing of George Floyd. For months after his death, official accounts repeatedly accused the United States of applying "double standards," particularly with respect for its support of Hong Kong protesters, highlighting allegations of police brutality. American politicians could "enjoy [the] sight [of protests] from their own windows," retorted the chief editor of state media outlet Global Times—a reference to US House Speaker Nancy Pelosi's comment that earlier Hong Kong protests were "a beautiful sight to behold."[76] In one particularly salient episode, China's Foreign Ministry spokeswoman responded to a tweet from the US State Department that called for solidarity with Hong Kong protesters with "I can't breathe," a reference to George Floyd's death.[77]

Both Russia and China invest large sums targeting overseas audiences

Russian state media and diplomatic accounts also leaned in to claims of US hypocrisy at this time, contrasting US promotion of human rights abroad with crackdowns on peaceful domestic protesters.[78]

Both Beijing and Moscow have built followings on Twitter by skillfully blending strategic messaging with content meant to connect with Western audiences. Russian state media outlets, for instance, frequently post cute animal videos and other human-interest content on Twitter.[79] They also make efforts to engage on viral topics with memes: during 2020 vote counting in Nevada, for example, RT posted multiple images featuring American celebrities and cartoon characters that poked fun at the delay in reporting results.[80] For China, this has included panda videos, clickbait content, and other digital memes designed to go viral.[81] This messaging reflects an understanding that a Twitter audience is a strategic asset.

Both Russia and China have deployed multiple, at times conflicting, conspiracies to deflect blame for their own activities and to undermine the notion of objective truth. After the poisoning of Sergei Skripal in the United Kingdom in March 2018, Russian outlets flooded the internet with alternative theories, assigning culpability variously to the United States, United Kingdom, a drone, and even the future mother-in-law of his also-poisoned daughter, Yulia.[82] More recently, a senior Chinese Foreign Ministry spokesman promoted the idea that the United States created the coronavirus as a biological weapon, citing a now-deleted post on a Kremlin-linked proxy website that focused suspicion on Fort Detrick, a US Army biological research facility in Frederick, Maryland. Both use official accounts on Twitter to amplify false theories—in the latter case, Beijing's diplomatic and state media accounts on Twitter have done so more than 880 times.[83]

These efforts have intensified since late May, when the Biden administration re-opened the investigation into a possible virus leak at the Wuhan Institute of Virology. As analyst Bret Schafer has noted, at least 35 Chinese officials and state media outlets mentioned Fort Detrick in more than 115 tweets in nine languages in the roughly six weeks that followed.[84] Beijing's willingness to traffic in conspiracy theories represents something of a departure from its earlier approach. Until this past year, China tended to be more risk averse, opting to suppress critical content rather than drown it out with false or conspiratorial messaging. But concern that China could be blamed for causing a pandemic that has claimed the lives of more than four million people and reaped significant economic dislocation worldwide may have changed Beijing's risk calculation.

Both Russia and China invest large sums in propaganda outfits that target overseas audiences. Facing new sanctions and declining popularity at home, Putin is reportedly aiming to expand the global audience of Kremlin-funded RT by 100 million viewers, including on online platforms, by promoting the

digital content of Russia's "entire fleet" of outlets—from RIA Novosti to Sputnik radio. To accomplish this task, he increased the budget for state media to roughly US$2.8 billion, an increase of more than US$400 million over previous years.[85]

Beijing, for its part, reportedly allocated US$6 billion to expanding state media globally as early as 2009.[86] Political scientist David Shambaugh estimated that the Party spends roughly US$10 billion a year on expanding its soft power generally.[87] And there is evidence that China's state media and associated entities recently paid to promote tweets designed to discredit Hong Kong protestors, even though Twitter is itself banned in mainland China.[88] Meanwhile, China's state media is building a substantial following on Facebook. According to a 2019 analysis by the Economist, Chinese state run news outlets CGTN, China Daily, People's Daily, and Xinhua have more Facebook followers than BBC News, CNN, and the New York Times.[89] These media properties provide a megaphone for state-proffered narratives.

Narratives: The Stories They Tell

Russia and China each promote narratives that advance their particular interests. Russia is focused on elevating divisive content designed to drive polarization up and social trust down, while pushing back on what it claims as anti-Russian bias. China, on the other hand, is primarily interested in touting the strength of its own governance model, while painting criticisms of its rights record as hypocritical. Both countries endeavor to erode confidence in the safety record of Western COVID-19 vaccines and cast the United States and its liberal democratic allies as ineffective.

Russia frequently promotes divisive themes designed to drive polarization, undermine confidence in democratic institutions, and denigrate democracy. A common refrain is that the Western media carries out censorship, whether by declining to cover important stories on vaccine safety (despite evidence to the contrary), or by excluding voices from the political left (part of a broader effort to exacerbate splits not just between the parties, but within the Democratic party).[90] After the Capitol riot and President Trump's removal from Facebook and Twitter, RT's promotion of anti-Big Tech narratives escalated, adopting partisan language and talking points from right- and some left-wing viewpoints alleging social media censorship, claiming that the platforms are politically biased, and arguing that purges of alternative viewpoints were imminent.[91] These narratives seek to dent democracy's appeal—to would-be activists at home, and to Americans—by casting it as hypocritical. Attacks on Big Tech may also be aimed at damaging some of the United States' most profitable companies,

while simultaneously making it more difficult for the United States to write the rules of the internet.

These messages are frequently accompanied by complaints of anti-Russian bias in US media, often amplifying domestic-origin "Russiagate" claims. For instance, Russian state media and diplomats portray the attribution of the SolarWinds hack as part of a US tradition of blaming Russia for its problems.[92] Following reports that Russian military intelligence offered bounties to the Taliban to attack coalition forces in Afghanistan, Russian state media and diplomats alleged that the story was a "new smear campaign" against Russia, a "hoax" planted by the CIA, and an effort to keep "Russiagate" alive.[93] A persistent theme in messaging about Russia's leading coronavirus vaccine, Sputnik V, alleges that Western mainstream media skepticism about it stemmed from anti-Russia bias, rather than any real concerns about the vaccine's development and approval process.[94]

China, meanwhile, promotes narratives that cast democracy as feckless, ineffective, or hypocritical and highlights the strength of its model, touting themes that are relevant to its geopolitical interests. In the spring of 2020, as the coronavirus pandemic spread across Europe, it worked to position itself as a partner of first resort to traditional US allies on the continent at a moment when the United States was hobbled. Chinese state and private donations of medical-grade masks to Europe early in the pandemic, for example, were accompanied by a substantial messaging push that advanced positive CCP concepts, such as a "shared future for mankind," as well as active denigration of European democracies to present China's authoritarian model as more effective.[95]

China also frequently paints the United States as hypocritical in its position on protesters with respect to Hong Kong. In a prominent example, Chinese diplomats and state media sought to draw a parallel between the Hong Kong protests and the US demonstrations that followed the killing of George Floyd, accusing the United States of having "double standards" for supporting the supposedly violent Hong Kong protestors while condemning violence during the US unrest.[96] More recently, Beijing's diplomats and state media have sought to counter accusations of genocide in Xinjiang by pointing to the treatment of Native Americans in the United States. In February, Beijing's two most prominent spokespeople posted near-identical tweets within minutes of each other suggesting that the United States is the true perpetrator of genocide.[97]

Both countries deploy narratives to undermine confidence in Western vaccines

In their efforts to highlight the political weaknesses of the West, both countries deploy narratives designed to undermine confidence in the safety and

viability of Western vaccines, highlight election chaos, troll the United States on its record of race and policing, and generally paint democracies as weak and ineffective. During the 2020 election cycle, Russian state media amplified various claims of voter fraud, irregularities, and general unfairness, while suggesting that the United States should not be held up as a model democracy.[98] Russian state media and diplomats alike also used the attack on the US Capitol to criticize US democracy.[99] China's state media extensively covered anticipated violence around President Biden's inauguration, making, as researchers Amber Frankland, Nathan Kohlenberg, Bret Schafer, and Etienne Soula write, "the implicit and explicit point that US exceptionalism is, and always has been, a myth."[100]

While not promoting verifiably false information, Russian state media emphasized adverse reactions to the Pfizer vaccine in coverage between November 2020 and February 2021, often implying a causal connection between the vaccine and later deaths while omitting or downplaying important context.[101] In China's promotion of its own vaccines, state media and diplomats indicated that their vaccines are meant for the "global public good," rather than profit, "which was implicitly or explicitly presented as the West's primary motivation."[102] Russian state media portrayed the February 2021 weather disaster in Texas, for instance, as evidence that the United States cannot protect its citizens and should direct more attention to its domestic issues than global issues like the Nord Stream 2 pipeline project.[103]

Anticipating What's to Come

From Russia, we are witnessing a shift away from the use of troll farm content toward harder to detect, more targeted information operations, likely carried out by Russian military intelligence. These operations cover wider ground within the information ecosystem, from search results manipulated by the exploitation of data voids to the statements of likely unwitting domestic political figures carried by established media.[104] This is partly driven by the evolution of platform detection mechanisms and other policies since Russia's 2016 operation caught the United States off guard. But it is also occurring for a more fundamental reason: Russia does not need large quantities of troll farm content to upend US domestic politics with divisive narratives that sow chaos, depress trust in institutions, and exacerbate social tensions. Americans are already doing that to themselves. This is perhaps the greatest coup of Russia's 2016 operation—it fueled a wave of partisan convulsions over election legitimacy that reverberates today.

2016 was somewhat of an inflection point for the Kremlin, since it simultaneously trained public attention on the threat of Russian interference,

increasing the likelihood of detection for certain forms of online operations, and ushered in a hyper-partisan era ripe for Russia's broader information manipulation activity in other forms. That has particularly included the use of real Americans to promote disinformation, as the US Intelligence Community's report on foreign interference in the 2020 election laid painfully bare.[105] But these changes are more an evolution, or shift in emphasis, than a dramatic break from past practice.

From China, we are witnessing a departure from its more subtle approach to information manipulation to one that is markedly more assertive and confrontational, carried out by a growing army of diplomats online. Since March of 2019, the number of official Chinese accounts on Twitter has grown nearly fivefold.[106] "Wolf warriors" promote outright conspiracies and troll Western officials. There was once scant evidence of coordination or strategy on the part of China's diplomatic corps—some important embassies (e.g., in the United Kingdom and United States) had no social media properties, while others of less obvious geopolitical relevance had prolific ones. Their messaging was not synchronous and seemed to operate without clear direction from Beijing. Today, that is no longer the case. This activity began in late March 2019, as the first pro-democracy protests filled Hong Kong's streets. Between September and December of that year, as the unrest escalated, Beijing created more than 60 new accounts, roughly one and half times more than it held in total earlier that spring.[107] Today, it operates more than 200.[108] The coronavirus—an issue of particular geopolitical salience to Beijing—only accelerated this growth. It has and will continue to provide new opportunities to put these assets to use.

China has shifted from a more subtle to an assertive and confrontational approach since March 2019

The United States and other liberal democracies need to develop a strategy to push back on these activities—one that appreciates that the information domain is a critical, but not the exclusive theater, of the emerging, asymmetric competition with authoritarians. This should emphatically *not* include responding to Russia and China's information manipulation with their own deceptive campaigns, as France was revealed to have done when Facebook took down a network of its trolls that were tangling with Russians in multiple countries in Africa late last year.[109] That approach would enable autocrats to dictate the terms of the competition and all but ensure that the contest will play out on terrain where democracies are at a strategic disadvantage.

Democracies should instead go on offense in the spaces most conducive to their success. In the information domain, this should entail applying the persistent engagement approach that they have developed for cyberspace, as analysts Laura Rosenberger and Lindsay Gorman have suggested, recognizing that there is an advantage to framing the debate.[110] It should include a concerted campaign, grounded in truthful information, to champion democracy and expose the failures of dictatorship.[111] And it should entail defending freedom of information, since transparency is a threat to Putin's and Xi's rule.[112] Ultimately, success in the information domain may require democratic governments to take action beyond it, leveraging other assets at their disposal. Democratic governments should do all of this in partnership with one another, recognizing that this is ultimately a contest over principles and that their strong network of alliances and partnerships is perhaps their greatest advantage. But the first step is for policymakers to develop a comprehensive, current threat picture to be able to anticipate what is to come.

Notes

1. Jessica Brandt, Zack Cooper, Bradley Hanlon, and Laura Rosenberger, *Linking Values and Strategy: How Democracies Can Offset Autocratic Advances* (Washington, DC: Alliance for Securing Democracy, November 5, 2020), https://securingdemocracy.gmfus.org/linking-values-and-strategy/.
2. Josh Rudolph and Thomas Morley, *Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies* (Washington, DC: Alliance for Securing Democracy, August 18, 2020), https://securingdemocracy.gmfus.org/covert-foreign-money/; "Authoritarian Influence Tracker," Alliance for Securing Democracy, accessed March 23, 2021, https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/.
3. Philip Zelikow, Eric Edelman, Kristofer Harrison, and Celeste Ward Gventer, "The Rise of Strategic Corruption: How States Weaponize Graft," *Foreign Affairs*, July/August 2020, https://www.foreignaffairs.com/articles/united-states/2020-06-09/rise-strategic-corruption.
4. Jessica Brandt and Torrey Taussig, "Europe's Authoritarian Challenge," *Washington Quarterly* 42, no. 4 (2019), 133–53, https://doi.org/10.1080/0163660X.2019.1693099; "Authoritarian Influence Tracker."
5. Christopher Walker, Shanthi Kalathil, and Jessica Ludwig. "The Cutting Edge of Sharp Power," *Journal of Democracy* 31, no. 1 (2020): 124–37, http://doi.org/10.1353/jod.2020.0010.
6. See, for example, the Alliance for Securing Democracy's Authoritarian Interference Tracker, accessed August 2021, https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/.
7. *GEC Special Report: Russia's Pillars of Disinformation and Propaganda* (Washington, DC: Department of State, 2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf; Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," Asan Forum, May 8, 2018,

http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/; Brian Hioe, "Moves By China to Train Taiwanese Influencers Are Unsurprising," New Bloom, https://newbloommag.net/2021/03/17/china-influencer-training/; Bradley Hanlon and Thomas Morley, "Russia's Network of Millennial Media," Alliance for Securing Democracy, February 15, 2019, https://securingdemocracy.gmfus.org/russias-network-of-millennial-media/; Miles Kenyon, "WeChat Surveillance Explained," Citizen Lab, May 7, 2020, https://citizenlab.ca/2020/05/wechat-surveillance-explained/; Jeanne Whalen, "Chinese Censorship Invades the U.S. via WeChat," *Washington Post*, January 7, 2021, https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/.

8. Brandt et al., *Linking Values and Strategy*.
9. Jessica Brandt, *How Democracies Can Win an Information Contest without Undercutting Their Values* (Washington, DC: Carnegie Endowment for International Peace, August 2, 2021), https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058.
10. Katherine Manstead, *Strong Yet Brittle: The Risks of Digital Authoritarianism* (Washington, DC: Alliance for Securing Democracy, May 28, 2020), https://securingdemocracy.gmfus.org/strong-yet-brittle-the-risks-of-digital-authoritarianism/.
11. Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs* 99, no. 3 (May/June 2020), https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.
12. "George Kennan's 'Long Telegram'," February 22, 1946, History and Public Policy Program Digital Archive, National Archives and Records Administration, Department of State Records (Record Group 59), Central Decimal File, 1945–1949, 861.00/2-2246, reprinted in *Foreign Relations of the United States*, US Department of State, ed., vol. VI (Washington, DC: Government Printing Office, 1969), 696–709.
13. Rosenberger, "Making Cyberspace Safe for Democracy."
14. "Gross Domestic Product 2019," World Bank Group, 2019, https://databank.worldbank.org/data/download/GDP.pdf.
15. "Russia's Economy Shrinks 3.1% in 2020, Sharpest Contraction in 11 Years," Reuters, February 1, 2021, https://www.reuters.com/article/russia-economy/russias-economy-shrinks-3-1-in-2020-sharpest-contraction-in-11-years-idUSL1N2K71M9; "Russia," OEC, accessed March 23, 2021, https://oec.world/en/profile/country/rus/; *Russia: Recession and Growth Under the Shadow of a Pandemic* (Washington, DC: World Bank Group, 2020), 43, https://openknowledge.worldbank.org/bitstream/handle/10986/34219/Russia-Recession-and-Growth-Under-the-Shadow-of-a-Pandemic.pdf.
16. Rosenberger and Garnaut, "The Interference Operations."
17. Rosenberger, "Making Cyberspace Safe for Democracy."
18. Rosenberger and Garnaut, "The Interference Operations"; Stephen Castle, "Former Russian Spy Mysteriously Falls Ill in Britain. Again," *New York Times*, March 5, 2018, https://www.nytimes.com/2018/03/05/world/europe/russian-spy-falls-ill-in-britain-again.html; Heidi Blake, *From Russia with Blood: The Kremlin's Ruthless Assassination Program and Vladimir Putin's Secret War on the West* (New York: Mulholland, 2019).
19. Mark Galeotti, "The 'Trump Dossier,' or How Russia Helped America Break Itself," Tablet, June 13, 2017, https://www.tabletmag.com/sections/news/articles/trump-dossier-russia-putin/; Mark Galeotti, "Russia Has No Grand Plans, But Lots of

'Adhocrats,'" Raam op Rusland, May 28, 2017, https://raamoprusland.nl/dossiers/het-kremlin/428-russia-has-no-grand-plans-but-lots-of-adhocrats.

20. Mark Galeotti, *Controlling Chaos: How Russia Manages Its Political War in Europe* (Berlin, European Council on Foreign Relations, 2017), https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/.
21. Indictment, *United States v. Internet Research Agency*, No. 1:18-cr-32 (D.D.C. February 16, 2018), Doc. 1, https://www.justice.gov/file/1035477/download; Andrew Radin, Alyssa Demus, and Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses* (Washington, DC: RAND, 2020), https://www.rand.org/pubs/perspectives/PE331.html; *GEC Special Report*.
22. Rosenberger and Garnaut, "The Interference Operations."
23. Jessica Brandt and Amber Frankland, *Leaks, Lies, and Altered Tape: Russia's Maturing Information Manipulation Playbook* (Washington, DC: Alliance for Securing Democracy, 2020), https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/; *Foreign Threats to 2020 US Federal Elections* (Washington, DC: Office of the Director of National Intelligence, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
24. "Chinese Economy to Overtake US 'by 2028' Due to Covid," *BBC*, December 26, 2020, https://www.bbc.com/news/world-asia-china-55454146.
25. *Global Competitiveness Report Special Edition 2020: How Countries are Performing on the Road to Recovery* (Cologny, Switzerland: World Economic Forum, 2020), https://www.weforum.org/reports/the-global-competitiveness-report-2020/in-full/infographics-14b60f7c60.
26. "How Developed Is China's Arms Industry?" ChinaPower (CSIS), February 18, 2021, https://chinapower.csis.org/arms-companies/.
27. Rosenberger and Garnaut, "The Interference Operations."
28. Liza Tobin, "Xi's Vision for Transforming Global Governance: A Strategic Challenge for Washington and Its Allies," *Texas National Security Review* 2, no. 1 (November 2018), https://repositories.lib.utexas.edu/bitstream/handle/2152/73730/TNSR_Vol_2_Issue_1_Tobin.pdf?sequence=2&isAllowed=y.
29. Matt Schrader, *Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries* (Washington, DC: Alliance for Securing Democracy, 2020), https://securingdemocracy.gmfus.org/friends-and-enemies-a-framework-for-understanding-chinese-political-interference-in-democratic-countries/.
30. Alex Ward, "How China's 'Wolf Warrior' Diplomats Use Twitter to Troll Beijing's Enemies," *Vox*, December 21, 2020, https://www.vox.com/22167626/china-wolf-warrior-twitter-online-interview.
31. Alex Joske, *The Party Speaks for You* (Canberra: Australian Strategic Policy Institute, 2020), https://www.aspi.org.au/report/party-speaks-you.
32. Schrader, *Friends and Enemies*.
33. Rosenberger and Garnaut, "The Interference Operations."
34. "China Media Group Signs Cooperation Agreement with Russian News Agency," *CGTN*, September 12, 2018, https://news.cgtn.com/news/3d3d774e7851544d7a457a6333566d54/share.html.
35. See the work of entities such as the Alliance for Securing Democracy, Digital Forensic Research Lab, Graphika, Institute for Strategic Dialogue, and Stanford Internet Observatory, among others. For example, Amber Frankland, Bret Schafer, Nathan

Kohlenberg, and Etienne Soula, *Influence-Enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives* (Washington, DC: Alliance for Securing Democracy, 2021), https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/; Nika Aleksejeva, Lukas Andriukaitis, Luiza Bandeira, Donara Barojan, et al., *Operation "Secondary Infektion": A Suspected Russian Intelligence Operation Targeting Europe and the United States* (DFRLab, August 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf; Ben Nimmo, Camille François, C. Shawn Eib, and L. Tamora, *From Russia with Blogs: GRU Operators Leveraged Blogs, Social Media Accounts and Private Messaging to Reach Audiences across Europe* (New York, Graphika, 2020), https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf; Raymond Serrato and Bret Schafer, *Reply All: Inauthenticity and Coordinated Replying in Pro-Chinese Communist Party Twitter Networks* (Washington, DC: Institute for Strategic Dialogue and Alliance for Securing Democracy, 2020), https://www.isdglobal.org/wp-content/uploads/2020/08/ISDG-proCCP.pdf; Raymond Serrato and Bret Schafer, *Reply All: Inauthenticity and Coordinated Replying in Pro-Chinese Communist Party Twitter Networks* (Washington, DC: Institute for Strategic Dialogue and Alliance for Securing Democracy, 2020), https://www.isdglobal.org/wp-content/uploads/2020/08/ISDG-proCCP.pdf.

36. See for example, among others: US Senate Select Committee on Intelligence, Russian Active Measures, Campaigns and Interference, *Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*, 116th Cong., 1st sess. (2019); US Senate Select Committee on Intelligence, Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election, *Volume 2: Russia's Use of Social Media with Additional Views*, 116th Cong., 1st sess. (2019); US Senate Select Committee on Intelligence, Russian Active Measures, Campaigns, and Interference in the 2016 US Election, *Volume 3: U.S. Government Response to Russian Activities*, 116th Cong., 2d sess. (2020); William Evanina, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, August 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public#:~:text=As%20I%20emphasized%20in%20my,the%20fabric%20of%20our%20democracy; Devlin Barrett, "FBI Director Affirms Russia's Aim to 'Denigrate' Biden Ahead of Election," *Washington Post*, September 17, 2020, https://www.washingtonpost.com/national-security/wray-fbi-election-security-threats-hearing/2020/09/16/4461526e-f869-11ea-a275-1a2c2d36e1f1_story.html.
37. For more detail on these and other tactics, see the author's 2020 paper, *Leaks, Lies, and Altered Tape: Russia's Maturing Information Manipulation Playbook* (Washington, DC: Alliance for Securing Democracy, 2020), https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/.
38. Michael Swirtz and Gaelle Borgia, "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader," *New York Times*, November 11, 2019, https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html.
39. Davey Alba and Sheera Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence," *New York Times*, October 30, 2019, https://www.nytimes.com/2019/10/30/technology/russia-facebook-disinformation-africa.html; Shelby Grossman, Daniel Bush, and Renée DiResta, "Evidence of Russia-Linked Influence Operations in Africa," Stanford

Internet Observatory, October 29, 2019, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

40. Michael Schwirtz and Sheera Frenkel, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *New York Times*, March 29, 2019, https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html/.
41. Ben Nimmo, Camille François, C. Shawn Eib, and L. Tamora, *From Russia With Blogs: GRU Operators Leveraged Blogs, Social Media Accounts and Private Messaging to Reach Audiences Across Europe* (New York, Graphika, 2020), https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf; Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar," Facebook Newsroom, February 12, 2020, https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/.
42. Tony Romm, Elizabeth Dwoskin, and Eli Rosenberg, "The Moment When Facebook's Removal of Alleged Russian Disinformation Became a Free-Speech Issue," *Washington Post*, August 1, 2018, https://www.washingtonpost.com/technology/2018/08/02/moment-when-facebooks-removal-alleged-russian-disinformation-became-free-speech-issue/.
43. Jack Stubbs, "Duped by Russia, Freelancers Ensnared in Disinformation Campaign by Promise of Easy Money," Reuters, September 2, 2020, https://www.reuters.com/article/us-usa-election-facebook-russia/duped-by-russia-freelancers-ensnared-in-disinformation-campaign-by-promise-of-easy-money-idUSKBN25T35E.
44. National Intelligence Council, *Foreign Threats to the 2020 U.S. Federal Elections* (Washington, DC: Office of the Director of National Intelligence, 2021).
45. Young Mie Kim, "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen," Brennan Center for Justice, March 5, 2020, https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more.
46. Bret Schafer, "The Hack-and-Leak Conundrum: There's No Good Way to Combat the Latest Form of Dirty Trick," *New York Daily News*, October 20, 2020, https://www.nydailynews.com/opinion/ny-oped-the-hack-and-leak-conundrum-20201020-egjuwbt7urbm3kyvqzswfmspka-story.html.
47. Ryan Brooks, "Real Black Activists Worry Fake Ones Will Drown Them Out on Twitter," *Buzzfeed*, February 27, 2019, https://www.buzzfeednews.com/article/ryancbrooks/black-activists-twitter-bots-2020-election-trolls.
48. Ben Collins, "A Russian Troll Farm Set an Elaborate Social Media Trap for the Midterms — and No One Bit," *NBC News*, November 7, 2018, https://www.nbcnews.com/tech/tech-news/russian-troll-farm-set-elaborate-social-media-trap-midterms-no-n933781.
49. NIC, *Foreign Threats to the 2020 U.S. Federal Elections*.
50. The Obama administration grappled with this dynamic in 2016. U.S. Congress, Senate, Select Committee On Intelligence, *Russian Active Measures, Campaigns, and Interference in the 2016 U.S. Election, Volume 3: U.S. Government Response to Russian Activities*, 116th Cong., 2d sess., 2020, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf.
51. NIC, *Foreign Threats to the 2020 U.S. Federal Elections*.

52. Kirill Meleshevich and Bret Schafer, *Online Information Laundering: The Role of Social Media* (Washington, DC: Alliance for Securing Democracy, 2018), https://securingdemocracy.gmfus.org/online-information-laundering-the-role-of-social-media/.
53. Hanlon and Morley, "Russia's Network of Millennial Media"; Ishmael N. Daro, "This Quirky New Viral Video Channel Is Funded By The Russian Government," *Buzzfeed*, December 15, 2016, https://www.buzzfeed.com/ishmaeldaro/quirky-viral-video-channel-is-funded-by-the-russian-govt.
54. *GEC Special Report*.
55. *GEC Special Report*
56. Michael Golebiewski and Danah Boyd, *Data Voids: Where Missing Data Can Easily Be Exploited* (Data & Society, 2019), https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf.
57. Olivia Solon, "How Syria's White Helmets Became Victims of an Online Propaganda Machine," *Guardian*, December 18, 2017, https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.
58. Bret Schafer, "PD Next – De-Mystifying Disinformation, Malign Influence, and the Current Information Environment Session," Presentation at PD Next 2019 Conference, November 6, 2019. See also: Olivia Solon, "How Syria's White Helmets Became Victims of an Online Propaganda Machine," *The Guardian*, December 18, 2017, https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.
59. See Ellen Nakashima et al, "FBI Was Aware Prominent Americans, Including Giuliani, Were Targeted by Russian Influence Operation," *Washington Post*, May 1, 2021, https://www.washingtonpost.com/national-security/rudy-giuliani-fbi-warning-russia/2021/04/29/5db90f96-a84e-11eb-bca5-048b2759a489_story.html; Jessica Brandt, "The 'Ukraine Did It' Conspiracy Theory Is Dangerous: Here's Why," *The Hill*, December 2, 2019, https://thehill.com/opinion/national-security/472555-the-ukraine-did-it-conspiracy-theory-is-dangerous-heres-why.
60. Brandt and Frankland, *Leaks, Lies, and Altered Tape*.
61. "Hamilton 2.0 Dashboard," Alliance for Securing Democracy, accessed March 24, 2021, https://securingdemocracy.gmfus.org/hamilton-dashboard/.
62. Alex Ward, "How China's "Wolf Warrior" Diplomats Use Twitter to Troll Beijing's Enemies," *Vox*, December 21, 2020, https://www.vox.com/22167626/china-wolf-warrior-twitter-online-interview; Brandt and Taussig, 2019; Jessica Brandt, "Beijing's Viral Disinformation Activities," Power 3.0, April 2, 2020, https://www.power3point0.org/2020/04/02/beijings-viral-disinformation-activities/.
63. For more detail on these and other techniques, see: Jessica Brandt and Bret Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter," Brookings, October 28, 2020, https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/.
64. "Cuba Cannot Get Swiss Respirators Due to US Inhuman Blockade," *teleSUR*, April 29, 2020, https://www.telesurenglish.net/news/Cuba-Cannot-Get-Swiss-Respirators-Due-to-US-Inhuman-Blockade-20200429-0013.html (article retweeted by Chinese columnist Chen Weihua, https://twitter.com/i/web/status/1255835919753641984); Chen Weihua (@chenweihua), "What a joke that the Worst Secretary of State Mike Pompeo wants to pretend he is UN Secretary General. And this ahead of the US General Assembly," Twitter, September 20, 2020, 11:56 a.m., https://twitter.com/i/web/status/1307710189823569920.

65. "Hamilton 2.0 Dashboard."
66. *GEC Special Report*.
67. Amber Frankland, Nathan Kohlenberg, Bret Schafer, and Etienne Soula, "Hamilton Toplines: February 22-28, 2021," Alliance for Securing Democracy, March 2, 2021, https://securingdemocracy.gmfus.org/hamilton-toplines-february-22-28-2021/.
68. Brandt and Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter."
69. Raymond Serrato and Bret Schafer, *Reply All: Inauthenticity and Coordinated Replying in Pro-Chinese Communist Party Twitter Networks* (Washington, DC: Institute for Strategic Dialogue and Alliance for Securing Democracy, 2020), https://www.isdglobal.org/wp-content/uploads/2020/08/ISDG-proCCP.pdf.
70. Brandt and Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter."
71. "Hamilton 2.0 Dashboard."
72. Brandt and Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter."
73. "Hamilton 2.0 Dashboard."
74. Lijian Zhao (@zlj517), "Welcome to Urumqi, the capital of Xinjiang, China," Twitter, September 29, 2020, 10:42 a.m., https://twitter.com/zlj517/status/1310953195808731138; Chinese Emb Pakistan (@CathayPak), "#Xinjiang stories: The Owner of Night Market Nurbiya Memet," Twitter, August 17, 2020, 3:03 a.m., https://twitter.com/CathayPak/status/1295254979868086272.
75. Jessica Brandt and Bret Schafer, "Five Things to Know about Beijing's Disinformation Approach," Alliance for Securing Democracy, March 30, 2020, https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.
76. Zhaoyin Feng, "George Floyd Death: China Takes a Victory Lap over US Protests," *BBC*, June 5, 2020, https://www.bbc.com/news/world-us-canada-52912241.
77. Hua Chunying (@SpokespersonCHN), "'I can't breathe.'" Twitter, May 30, 2020, 10:43 a.m., https://twitter.com/SpokespersonCHN/status/1266741986096107520.
78. Amber Frankland, Bret Schafer, and Etienne Soula, "Hamilton Weekly Report: May 23-29, 2020," Alliance for Securing Democracy, June 2, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-may-23-29-2020/; Amber Frankland, Bret Schafer, and Etienne Soula, "Hamilton Weekly Report: May 30-June 5, 2020," June 9, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-may-30-june-5-2020/.
79. Recent examples include RT (@RT_com), "He might look cute, but he just woke up and probably super hungry!" Twitter, March 19, 2021, 9:00 a.m., https://twitter.com/RT_com/status/1372895638044639232; RT (@RT_com), "I'm going deep! | Russian freediver sets new world record," Twitter, March 19, 2021, 11:00 a.m., https://twitter.com/RT_com/status/1372925834550407172; Ruptly (@Ruptly), "#Kashmiri goat was seen engaging in a mischievous stand-off-ish incident with a car," Twitter, March 19, 2021, 9:30 a.m., https://twitter.com/Ruptly/status/1372903183035609097; Sputnik (@Sputniklnt),"Watch how Indian Bhangra dancers wished the Irish a Happy St Patrick's Day," Twitter, March 19, 2021, 8:21 a.m., https://twitter.com/SputnikInt/status/1372885816335335426.
80. RT (@RT_com), "The dankest memes on #Nevada's crazy long delay in counting the votes #Election2020," Twitter, November 6, 2020, 8:00 a.m., https://twitter.com/RT_com/status/1324698052133867520.
81. Global Times (@globaltimesnews), "#Blackpink's #LISA set the stage ablaze with a #CollaborativePerformance," Twitter, May 24, 2020, 10:36 a.m., https://twitter.com/globaltimesnews/status/1264565902114058242; Ambassador Deng Xijun

(@China2ASEAN), "A #giantpanda at the zoo in Dalian, Liaoning, China interacting with tourists," Twitter, August 30, 2020, 3:59 a.m., https://twitter.com/China2ASEAN/status/1299979978642087938.

82. Ellen Barry, "At Site of U.K. Poisoning, Doubts About Case Creep In," *New York Times*, June 16, 2018, https://www.nytimes.com/2018/06/16/world/europe/uk-skripal-russia-salisbury-propaganda.html.
83. "Hamilton 2.0 Dashboard."
84. Bret Schafer, "China Fires Back at Biden with Conspiracy Theories about Maryland Lab," *Foreign Policy*, July 9, 2021, https://foreignpolicy.com/2021/07/09/china-fires-back-at-biden-with-conspiracy-theories-about-maryland-lab/.
85. Anna Nemtsova, "Putin Ramps Up RT's Propaganda Budget as Poll Rating Slumps," Daily Beast, March 5, 2021, https://www.thedailybeast.com/putin-ramps-up-rts-propaganda-budget-as-poll-rating-slumps.
86. "Beijing in 45b Yuan Global Media Drive," *South China Morning Post*, January 12, 2009, https://www.scmp.com/article/666847/beijing-45b-yuan-global-media-drive; Sarah Cook, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017* (Washington, DC: Freedom House 2020), https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone#footnoteref2_ewqyefj.
87. "China Is Spending Billions to Make the World Love It," *The Economist*, March 25, 2017, https://www.economist.com/china/2017/03/23/china-is-spending-billions-to-make-the-world-love-it; Cook, *Beijing's Global Megaphone*.
88. "China's Propaganda Machine Is Spending over $1 Million to Buy Influence on Foreign Social Media," Quartz, August 21, 2019, https://qz.com/1691785/chinas-paying-to-build-its-influence-on-foreign-social-media/.
89. "China Is Using Facebook to Build a Huge Audience around the World," Economist, April 20, 2019. https://www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world.
90. Bret Schafer, "Censorship and the Capitol Riot: How Big Tech Became the Target of Russian, Chinese, and Iranian Messaging," Alliance for Securing Democracy, January 22, 2021, https://securingdemocracy.gmfus.org/censorship-and-the-capitol-riot-how-big-tech-became-the-target-of-russian-chinese-and-iranian-messaging/; "Silencing Discussion? UK Labour Party Demands Online Crackdown on 'Anti-Vax Disinformation' Ahead of Covid-19 Vaccine Rollout," RT, November 15, 2020, https://www.rt.com/uk/506806-labour-vaccine-disinformation-censorship/; Tim Mak, "How Russia Is Trying To Boost Bernie Sanders' Campaign," *NPR*, March 5, 2020, https://www.npr.org/2020/03/05/812186614/how-russia-is-trying-to-boost-bernie-sanders-campaign.
91. "Ex-Facebook Exec Calls For De-Platforming OANN and Newsmax, Laments That Some Conservatives Have Bigger Audiences Than CNN," RT, January 17, 2021, https://www.rt.com/usa/512819-facebook-exec-deplatform-oann-newsmax/; RT (@RT_com), "Who will Twitter's purge campaign target next?" Twitter, January 15, 2021, 1:45 a.m., https://twitter.com/RT_com/status/1349970823474417664; Soapbox (@soapbox_soapbox), "Elites are exploiting a political crisis to get you to cheer for censorship," Twitter, January 12, 2021, 7:28 p.m., https://twitter.com/soapbox_soapbox/status/1349151203482071042.
92. Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Etienne Soula, "Hamilton Toplines: December 12-18, 2020," Alliance for Securing Democracy, December 22, 2020, https://securingdemocracy.gmfus.org/hamilton-toplines-december-12-18-2020/.

93. Amber Frankland, Bret Schafer, Nathan Kohlenberg, Etienne Soula, "Hamilton Weekly Report: June 27-July 3, 2020," Alliance for Securing Democracy, July 7, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-june-27-july-3-2020/.
94. Amber Frankland, "Hamilton Analysis: The Vaccine Race: Russia's Coverage of the Sputnik V Announcement," Alliance for Securing Democracy, August 18, 2020, https://securingdemocracy.gmfus.org/hamilton-analysis-the-vaccine-race-russias-coverage-of-the-sputnik-v-announcement/; Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Etienne Soula, *Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives* (Washington, DC: Alliance for Securing Democracy, 2021), https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/; Pjotr Sauer and Jake Cordell, "'Gross Violation': In Open Letter, Russian Scientists Criticize Lack of Vaccine Data," *Moscow Times*, December 10, 2020, https://www.themoscowtimes.com/2020/12/10/gross-violation-in-open-letter-russian-scientists-criticize-lack-of-vaccine-data-a72311.
95. Etienne Soula, Franziska Luettge, Melissa Ladner, and Manisha Reuter, *Masks Off: Chinese Coronavirus Assistance in Europe* (Washington, DC: Alliance for Securing Democracy and GMF Asia Program, 2020), 7–11, https://securingdemocracy.gmfus.org/wp-content/uploads/2021/03/ASD-ASIA-EU-China-Coronavirus-final.pdf.
96. Amber Frankland, Bret Schafer, Etienne Soula, "Hamilton Weekly Report: May 23-29, 2020," Alliance for Securing Democracy, June 2, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-may-23-29-2020/; Amber Frankland, Bret Schafer, Etienne Soula, "Hamilton Weekly Report: May 30-June 5, 2020," Alliance for Securing Democracy, June 9, 2020, https://securingdemocracy.gmfus.org/hamilton-weekly-report-may-30-june-5-2020/.
97. Amber Frankland, Nathan Kohlenberg, Bret Schafer, and Etienne Soula, "Hamilton Toplines: February 22-28, 2021," Alliance for Securing Democracy, March 2, 2021, https://securingdemocracy.gmfus.org/hamilton-toplines-february-22-28-2021/.
98. Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Bryce Barros, "Hamilton Toplines: October 24-30, 2020," Alliance for Securing Democracy, November 3, 2020, https://securingdemocracy.gmfus.org/hamilton-toplines-october-24-30-2020/; Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Etienne Soula, "Hamilton Toplines: October 31-November 6, 2020," Alliance for Securing Democracy, November 10, 2020, https://securingdemocracy.gmfus.org/hamilton-toplines-october-31-november-6-2020/; Bret Schafer, "Foreign Amplification of Voter Fraud Narratives: How Russian, Iranian, and Chinese Messengers Have Leveraged Post-Election Unrest in the United States," Alliance for Securing Democracy, November 24, 2020, https://securingdemocracy.gmfus.org/foreign-amplification-of-voter-fraud-narratives-how-russian-iranian-and-chinese-messengers-have-leveraged-post-election-unrest-in-the-united-states/.
99. Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Etienne Soula, "Hamilton Toplines: January 2, 2021-January 8, 2021," Alliance for Securing Democracy, January 12, 2020, https://securingdemocracy.gmfus.org/hamilton-toplines-january-2-2021-january-8-2021/.
100. Amber Frankland, Bret Schafer, Nathan Kohlenberg, Etienne Soula, "Hamilton Toplines: January 2, 2021-January 8, 2021," Alliance for Securing Democracy, January 12, 2020, https://securingdemocracy.gmfus.org/hamilton-toplines-january-2-2021-january-8-2021/.

101. Frankland et al., *Influence-enza*; Nebojsa Malic, "What Happened to Facts and Science? Western Propaganda about 'Vaccine Disinformation' Is Just Another Russiagate," RT, March 8, 2021, https://www.rt.com/op-ed/517549-russia-vaccine-propaganda-biden/.
102. Frankland et al., *Influence-enza*.
103. Amber Frankland, Bret Schafer, Nathan Kohlenberg, and Etienne Soula, "Hamilton Toplines: February 15-21, 2021," Alliance for Securing Democracy, https://securingdemocracy.gmfus.org/hamilton-toplines-february-15-21-2021/.
104. Brandt and Frankland, *Leaks, Lies, and Altered Tape*.
105. NIC, *Foreign Threats to the 2020 U.S. Federal Elections*.
106. "Hamilton 2.0 Dashboard."
107. "Hamilton 2.0 Dashboard."
108. "Hamilton 2.0 Dashboard."
109. Hannah Murphy and Sid Venkataramakrishnan, "Facebook Finds French and Russian Trolls Sparring in Africa," *Financial Times*, December 15, 2020, https://www.ft.com/content/b4de10c7-c391-4c59-b7ff-c5c3770752de.
110. Laura Rosenberger and Lindsay Gorman, "How Democracies Can Win the Information Contest," *Washington Quarterly* 43, no. 2 (2020), 75–96, https://doi.org/10.1080/0163660X.2020.1771045.
111. Daniel Twining and Patrick Quirk, "Winning the Great Power Competition Post-Pandemic," *American Interest*, May 11, 2020, https://www.the-american-interest.com/2020/05/11/winning-the-great-power-competition-post-pandemic/.
112. Brandt et al., *Linking Values and Strategy*.