The Evolution of Authoritarian Digital Influence

Grappling with the New Normal

By Shanthi Kalathil

As the world contends with the wide-ranging ramifications of the global COVID-19 pandemic, it has been simultaneously beset by the global information crisis, which mimics the shape of the pandemic itself in its viral effects across huge segments of the global population.

Misinformation—unwittingly spread false information—is rampant. Overarching narratives, targeted propaganda, and particularly disinformation—the deliberate generation of false or misleading information designed to engender public cynicism or uncertainty—are being piped into the global information bloodstream in large quantities. While some of this comes from domestic political actors, determined authoritarian regimes and their proxies have been quick to seize this window of opportunity for asymmetric transnational impact. Many of those targeted, including governments, institutions, and segments of societies, have been too overwhelmed to respond effectively.

These networked, cross-border influence operations by authoritarian actors have grown in sophistication and effectiveness in recent years,[1] shaping narratives and targeting democratic institutions during important geopolitical moments.[2] While not disavowing more traditional forms of propaganda, authoritarian regimes are increasingly using digital influence operations as a method of censorship and manipulation, flooding the information space[3] with false or misleading narratives designed to crowd out independent voices and expertise. Their motivations may be as narrow as seeking to muddy facts around particular incidents, or as broad as endeavoring to damage institutions and social cohesion in democracies[4] by exploiting and amplifying social, political, and economic vulnerabilities.[5] There is increasing evidence that authoritarian networks are amplifying, cross-pollinating,[6] and learning from one another.[7] Key authoritarian state and state-linked actors in this space include those from the People's Republic of China (PRC), Russia, Iran, Saudi Arabia, Venezuela, and others.[8]

But while the current moment shows these patterns in stark relief, this is not a new dynamic. Over the past several years, such challenges emanating from the networked, global information ecosystem have moved to the heart of great power competition for the United States and other democracies around the world. While this is slowly prompting a rethink of the typical national security toolkit, democratic governments remain back-footed and hampered by lack of capacity and broader coordination. Existing structures, policy processes,

Shanthi Kalathil is the Senior Director of the International Forum for Democratic Studies at the National Endowment for Democracy.

and prescriptions have yet to catch up with the scale of the challenge. Meanwhile, authoritarian regimes use the current chaotic moment to fine-tune their global approaches and press their advantage. The non-governmental sector (including media and tech platforms) and the broader public represent both a soft target as well as a source of resilience—yet are not fully integrated into policy conversations and potential solutions.

In a time of growing distrust of institutions—and doubts about democracy's capacity to deliver—authoritarian regimes are no longer content to quell democratic stirrings within their own borders. In ways subtle and overt they are actively using the global information space to take aim at the values and institutions undergirding the rules-based international order, discrediting the idea of democracy, and attempting to weaken key democratic norms. Far from merely aiming at boosting approval ratings at home and abroad, for them this is an existential question about the survival of their governance systems, and the values that should underpin the international system going forward.

This article examines recent trends and developments in authoritarian regimes' transnational digital influence operations, particularly in light of the COVID-19 pandemic. It will address changes in the information environment that have proved fertile for such operations, the methods and goals of key players in this space, and provide insight on ways that democratic governments can update their own thinking and processes to increase resilience and capacity.

Digital Influence Operations

A number of terms have been used to describe a range of activity in the information space; hybrid warfare, psychological warfare, active measures, fake news, disinformation, propaganda, coordinated inauthentic behavior, information/influence operations. While not interchangeable, they all describe a range of interrelated malign activity, intended to mislead or deceive, in the global information space. For the purposes of this article, the term "digital influence operations" will be used to broadly capture the categories of digital activity most commonly employed by authoritarian regimes internationally to manipulate, censor, and degrade the integrity of the information space for strategic purposes.

While these efforts take place in the digital space and are deeply networked, they are not limited to "bots," or automated online programs. Due to widespread bot activity during democratic elections around the world in recent years, the perception that inauthentic coordinated activity forms the entirety of such efforts can lead to poorly aimed responses. In fact, authoritarian digital influence efforts leverage all elements of the information space, including through ownership of online media outlets and tech platforms, business and advertising pressure, and traditional censorship techniques. In the case of the PRC in particular, this extends to a wide spectrum of efforts designed to influence the architecture, norms, and governance of the global information space in a direction that favors the Chinese Communist Party (CCP)[9] and a related restriction of free expression, distinguishing this from efforts by democratic governments.

To narrow the scope of inquiry, this essay will limit its examination to the motivations and methods of transnational authoritarian digital influence operations. It will not examine purely domestic authoritarian campaigns to crack down on homegrown dissent or manipulate information. Similarly, it will not seek to address authoritarian regimes' cyber exploits including hacking or other intrusions, but recognizes that these elements frequently go together[10] with digital influence operations and complement each other. Finally, while the role of major tech platforms in facilitating disinformation is a vast and related research issue, it is beyond the ambit of this essay to thoroughly address, except to

acknowledge that without a robust response from the world's tech platforms, other efforts to combat authoritarian digital influence operations are not likely to be as effective.

A Fertile Environment for Digital Influence Operations

Changes in the information environment have in some ways enhanced authoritarian regimes' abilities to deploy transnational digital influence operations, even as traditional aspects of democratic resilience (such as financially sustainable independent media) have degraded. Over the past decade, the global information space has been characterized by greater connectivity, speed, and (in some instances) transparency, but also hyper-volatility,[11] the decline of traditional and trusted intermediaries (such as local news outlets or key editorial positions), and widespread media capture.[12] Moreover, the explosive growth in connectivity over the past decade and a half has also coincided with a resurgence in globally assertive authoritarianism as well as backsliding on key political and civil rights in a number of countries (what some have termed the democratic recession).[13]

It is notable, however, that whereas in the past it was assumed that democracy would clearly benefit from a more democratized, decentralized information space with fewer gatekeepers, this has not necessarily materialized. In fact, some of democracies' traditional strengths have become weaknesses in the new environment. Commercial competition among media providers used to be thought a determinant in enhancing the quality and credibility of competition; however, in the current environment, struggling independent, for-profit media can be and are frequently competing not only against each other but also against outlets (in both the physical and digital space) that are bankrolled by free-spending, authoritarian governments, or those affiliated with them. Not only does this present an uneven playing field, but commercial pressures may also lead outlets to relax editorial scrutiny of outside contributors, who may be concealing business interests linking them to authoritarian governments.[14] Disinformation outlets may also disguise themselves as independent journalism while failing to adhere to standard, best-practice accountability measures, such as bylines, mastheads, verification, corrections, and community service principles. Meanwhile, real news generation atrophies because platforms have absorbed the revenue of local independent journalism.[15] All of this can facilitate the success of authoritarian regimes' strategies to disrupt and subvert the information systems of targeted countries and regions.[16]

This has been paralleled by the rise of the "attention economy," which monetizes clicks and can drive information consumers toward particularly viral or sensational pieces of content.[17] Even as major technology platforms monetize attention, they maximize the data gathered from individual users, what some have called the surveillance capitalism model,[18] which can have strong negative implications for individual privacy[19] and create openings for authoritarian practices. The collection of vast amounts of data on individuals can enable precision microtargeting of messages, offering a potential goldmine for purveyors of disinformation. This combination can create a perfect storm of opportunity for authoritarian regimes and others who exploit these opportunities, including, for instance, the black market for attention (demonstrated by NATO studies of paid fake engagement on social media platforms).[20] As Ronald Deibert has summarized, the algorithms underlying social media also propel authoritarian practices that can facilitate manipulation, undermine accountability, and enable surveillance that can act as a proxy for authoritarian control.[21]

While it is not only authoritarian regimes that are able to manipulate the current information environment—far from it, as authoritarian-leaning populists from backsliding democracies

demonstrate—it is striking that studies of state actors employing such tactics highlight the prominent role played by major authoritarian regimes such as China and Russia. The Oxford Internet Institute's (OII) recent inventory[22] of organized social media manipulation highlights not only authoritarian regimes' growing capabilities to harness the information space within their own borders, but notes that around the world, there has emerged a key handful of sophisticated state actors who have been able to use computational propaganda for foreign influence operations. This handful consists of seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela), five of which are ranked as "Not Free" (and one as "Partly Free") by Freedom House's comprehensive measure of civil and political rights.[23] OII gives special mention to the PRC as having become a major player in the global disinformation order, whose aggressive use of Facebook, Twitter, and YouTube should raise concerns for democracies.[24] As noted further on in this article, these techniques have expanded and explored new modalities since the onset of the COVID-19 pandemic.

It should be noted that while authoritarian regimes can frequently be the source of global digital influence operations, the viral spread of disinformation requires person-to-person transmission; that is, there must be a demand for bad or misleading information that matches the supply. Analysis of why information consumers consume the content they do, and in particular why they may seek out and share misleading content for emotional or ideological validation, is important to understanding the broader dynamics behind the spread of disinformation in the current environment.[25] The answer may be linked to the psychology of news consumption and opinion formation. Research shows that across geographic contexts, deeply polarized societies with low trust in the media may be more susceptible to these psychological drivers behind consumption of misinformation or disinformation.[26] All of this has implications for response, as noted below.

Illustrative Tactics and Methods of Authoritarian Digital Influence Operations

Individual countries have differing strategic objectives and have pioneered different tactics, but they have also sought to pull best practices from each other and amplify each other when it serves their purposes. Many authoritarian regimes have a common interest in not merely burnishing their own images internationally, but in sowing distrust in democracy and the rule of law generally. Discrediting democracy as a governance model is a goal that all authoritarian regimes share, and the cost of doing so through the tactics described here has grown radically cheaper in recent years. Moreover, for many authoritarian regimes, control of information and narrative is seen as key to regime security, and inextricably bound up in their foreign policies. The following section highlights some key countries' digital influence tactics and operations, but is by no means meant to be exhaustive.

Innovations in Disinformation: Russia

Various aspects of Russian digital influence operations across North America, Europe, and beyond are now well known, and appear to have served as a model for other authoritarians' efforts. Many are now familiar with the Kremlin's attempts to utilize the information space to propel disinformation, sow distrust, promote polarization, and disrupt elections, particularly in the immediate run-up to the U.S. 2016 presidential election. Yet these efforts did not start there, nor did they end there. As some have noted, Russia's much-vaunted Internet Research Agency, run by a key Putin ally, originally was set up to manipulate domestic discourse within Russia.[27] Such efforts then moved outward, gradually being tested in near-abroad environments such

as Ukraine, before being deployed successfully in countries much farther afield. These activities may have been put in place well before any elections: Studies have found that Russian digital influence operations on platforms such as Twitter may have been set up and running well in advance of key election dates, speaking to foresight and planning as well as a long-term approach.[28]

Contrary to some perceptions, these operations do not rely solely on perpetuating overt falsehoods. Key tactics employed by Russian military intelligence (GRU) and others have included, according to a Stanford study, the updating for the digital age of such longstanding tactics as narrative laundering (legitimization of created narratives through repetition citations across media), and boosterism (repetitive content reinforcing the perception that a certain narrative represents a popular point of view). The digitization of old methods, according to the Stanford study, includes creation of online sock puppets, front websites purporting to be independent media, byline placement in politically aligned outlets, and dissemination and amplification via social networks. [29]

These tactics have been applied across weak and backsliding democracies, as well as more authoritarian environments, often in instances less well-known than the much publicized efforts surrounding the 2016 U.S. elections. In Turkey, for instance, censorship and manipulation already characterize the domestic information environment and render it susceptible to digital influence operations from the outside, including from Russia. Some argue that in addition to common strategies such as boosting both government and opposition narratives to foster division, pro-Russian digital influence operations in Turkey use a "forced perspective" approach that relies not on falsehoods, but on manipulating accurate information in order to remove context and distort the public narrative in favor of Russia's objectives.[30] Meanwhile, emerging studies on Russian digital influence operations across sub-Saharan Africa appear to show operations relying on private chat channels, as well as native-speaker local subcontractors, adding a wrinkle to attribution of disinformation campaigns.[31]

Growing Sophistication: Iran

Iran's transnational digital influence operations have only in recent years come to the attention of the broader security and international affairs community. Analysis by the Atlantic Council notes that Iranian sock puppets, operating as early as 2010, have grown exponentially in recent years, with Facebook identifying (as of early 2020) approximately 2,200 assets directly affecting six million users, and 8,000 Twitter accounts responsible for roughly 8.5 million messages. These information operations, according to the Atlantic Council, have typically contrasted with Russian tactics; rather than sowing disinformation, they have tended to exaggerate Iran's moral authority while minimizing Iran's repression of its citizens.[32] As is the case with Russia and other authoritarian regimes, the Iranian approach is informed by the government's domestic experience with social media censorship and manipulation, particularly in the aftermath of the 2009 Green Movement protests, but with more sophisticated techniques being deployed domestically in more recent years. For instance, during the January 2018 nationwide protests, Twitter bots attempted to discredit widely shared videos of rallies, while pro-regime accounts guided protestors to the wrong locations and sought to convey that protests were small and localized.[33]

This growing sophistication has translated to past and ongoing transnational digital influence operations.[34] FireEye Threat Intelligence has identified networks of English-language social media accounts, thought to be organized in support of Iranian political interests, engaging in inauthentic behavior, with several of those and related accounts

subsequently removed by Facebook, Instagram, and Twitter in early 2020. According to FireEye, the broader network has leveraged authentic media content to promote desired political narratives that align with Iranian interests.[35]

Targeted Harassment: Saudi Arabia

Saudi Arabia's harassment of journalist Jamal Khashoggi prior to his murder is well known, but such attacks reportedly formed just a part of a broader pattern of troll farm-generated harassment of critics, dissidents, and others. According to OII, externally focused Twitter bot networks and disinformation increased following Khashoggi's murder in October 2018, seeking to cast doubt on key Saudi officials' roles in the murder, but other activities include posting of pro-government messages, inflammation of sectarian tensions, and targeting of key rivals.[36] According to the *New York Times*, Saudi operatives have been particularly active on Twitter, which has been used widely for news in the country since the Arab Spring uprisings.[37] Analysis of a December 2019 takedown of 88,000 Twitter accounts managed by Smaat, a digital marketing company based in Saudi Arabia, showed links to "a significant state-backed information operation" that combined commercial content with attacks on critics of the Saudi regime and criticism of Qatar, Iran, and Turkey.[38] Among its neighbors, Saudi Arabia is hardly singular for engaging actively in digital influence operations; half of the 12 countries identified by the OII as expending considerable human and financial resources on digital influence operations were from the Middle East, including Egypt, Iran, Israel, Saudi Arabia, Syria, and the UAE.[39]

Expanding Through the Broader Information Ecosystem: China

Until relatively recently, the Chinese Communist Party's (CCP) digital influence operations were considered relatively minimalist and ineffective, limited to tweeting harmless and obvious propaganda through official social media channels. This itself has been a misunderstanding of the CCP's full approach, as the party's longstanding effort to influence the global information environment has been multifaceted and directed simultaneously at infrastructure, governance, norms, standards, and technological development—all in addition to projecting disinformation and shaping broader narratives through journalism training and exchanges, content linkups, and leverage over private business.[40] In this sense, its digital influence goals are uniquely broad and ambitious, representing an effort to reshape the structure of the internet and emerging technology.[41]

While this article does not dwell at length on the PRC's longstanding efforts to reshape norms, platforms, technological development, and governance through both state action and the private sector, it is important to note that such activities surround and predate[42] the more public digital influence tactics that have been on more recent display. Recent elections in Taiwan and the Hong Kong protests for democracy proved a key inflection point for understanding the Chinese party-state's evolving and more complex approach to digital influence operations. While the official digital footprints of Chinese state media accounts can be overt in their propaganda, *sub rosa* digital influence operations have taken aim at the legitimacy of the Hong Kong protests, at the credibility of the protestors themselves, and at the integrity and legitimacy of the Taiwan elections and individual candidates.[43] Analysis conducted by the Australian Strategic Policy Institute of a 2019 network targeting the Hong Kong protests that was subsequently taken down by Twitter found that while the specific information operation appeared relatively hastily put together and unsophisticated, there was evidence that the network had been repurposed from earlier accounts—demonstrating that actors linked to the Chinese government may have been running covert

digital influence operations on western social media platforms for at least two years prior.[44]

None of this is to say that the official digital footprint of state media is ineffective—far from it. While some point to the unsubtle regurgitation of CCP talking points, there is growing evidence that such outlets are gaining in credibility and reach. As the *Economist* points out, the English-language Facebook page of state broadcaster CGTN is followed by 77 million, the most of any news site; the PRC also runs five of the six media outlets with the biggest Facebook followings, and if current growth continues Chinese state media may attract more followers in the coming years than even the most popular sports and entertainment celebrities in the world.[45]

It is important to note that the PRC's digital influence operations are not limited to western-originated platforms such as Facebook and Twitter. Chinese internet companies are now among the biggest in the world, and they provide potentially powerful alternate platforms to those from Silicon Valley—often with more obscure and less rights-protecting content policies and algorithms, data privacy practices, and governance structures,[46] governed within a PRC system where the Party is above the rule of law. Even companies that may wish to act independently are constrained by the pressures placed on the private sector within the PRC. There is evidence that platforms originating in China are pressured to hew to CCP content guidelines—even outside of China's borders, as evidenced by censorship[47] and manipulation on, among others, globally popular Chinese-owned social media platform TikTok.[48]

Meanwhile, as WeChat grows in popularity throughout the world, politicians and others in democracies are increasingly using it for political speech,[49] even given widespread evidence of content censorship along CCP guidelines.[50] Politically motivated censorship and manipulation of content on Chinese-owned platforms is typically not considered to be a "digital influence operation" in the classic sense, but it is likely that these less noticeable forms of content manipulation, aiming to delete topics sensitive to the CCP from the global conversation, will become even more prevalent if China's technology aims and presence continue on their current trajectory.[51]

Digital Influence Operations: Supercharged by COVID

The coronavirus pandemic has provided a significant window of opportunity for heightened digital influence operations, allowing authoritarian regimes to exploit information ecosystem weaknesses to drive disinformation while mutually amplifying and reinforcing narratives related to overarching strategic goals. While authoritarian regimes are not the only ones taking advantage of confusion, panic, and misleading information during this crisis, they have been able to leverage their skill at censorship and information manipulation within their own borders to ample effect beyond them, particularly while institutions that might hold them to account are occupied elsewhere. On the other side of this "supply" of the equation, the psychological factors behind the "demand" side of the so-called "infodemic" may drive even greater disinformation virality among large segments of the population, particularly during the current crisis.[52]

New research from the OII on misinformation and disinformation around the coronavirus pandemic indicates a high degree of reach for authoritarian information, with content from the state-backed, English-language outlets of the PRC, Russia, Iran, and Turkey reaching audiences of millions around the world. The study found that while these outlets produce less content than more independent outlets, they can achieve ten times the amount of effective engagement—all while pushing conspiracy theories and discrediting democracy.[53]

Instances of prevalent disinformation, propaganda, conspiracy theory, and misleading narratives have proliferated. These have included (inter alia); that the coronavirus is a biological weapon deployed by either China, the United States, or the UK; that the virus originated in the United States or Italy rather than in China; that migrants are spreading the virus; that the virus is linked to 5G; that the entire virus is a hoax; and that the virus is linked to longstanding conspiracy theories regarding "chemtrails" and similar narratives. [54]

In Latin America rumors have spread that the virus was engineered to spread H.I.V., while in Iran it is portrayed as a western plot.[55] While it can be difficult to disaggregate organically spread misinformation from directed digital influence operations, several specific examples can be attributed to existing major entities in this space.

Thank you, Putin. Thank you, Russia

Unsurprisingly, the dominant authoritarian players in digital influence operations have parlayed their existing innovation and success into more widespread manipulation of information during the global pandemic. The Kremlin, for instance, has not only continued but deepened its strategy of amplifying divisions, sowing distrust, and exacerbating crises.[56] According to a report by the European Union's External Action Service, Russia's RT Spanish is among the top-20 most engaged sources on major platforms on subjects related to the coronavirus. Moreover, the report found the Kremlin's disinformation strategies targeting international audiences to focus primarily on conspiracy theories regarding global elites exploiting the virus, aimed at creating distrust in national and European healthcare systems, institutions, and scientific experts.[57]

The Kremlin has used the crisis to further drive disinformation in support of strategic objectives, such as exacerbating anti-NATO sentiment among Eastern European audiences. In Lithuania, a legitimate news site was hacked to post a false story claiming a U.S. soldier there had contracted the virus, while pro-Russian news outlets have claimed Lithuanian authorities would be shutting down pro-Russian media outlets, for instance, or that strategic food reserves had been destroyed.[58] Beyond Eastern Europe, the Kremlin has been active in countries hit hard by the pandemic, including Italy, where the information environment has already been dominated by domestically generated and spread misinformation and disinformation. According to the Atlantic Council's DFR Lab, the Kremlin's "from Russia with love" message has accompanied shipments of medical supplies and experts, with supporting narratives amplified in both Russia and Italy. Social media content has included a YouTube video titled "Russia tries to help Italy. But is someone mysteriously boycotting it," watched by more than 25,000 people and liked over 8,000 times; meanwhile, images surrounding aid transport insinuated that EU countries were obstructing help from Russia. Such images were accompanied by hashtags #italexit and #uscITA, supporting Italy leaving the EU.[59] While these campaigns bear similarities to past information operations, the chaotic and saturated information environment surrounding the pandemic may help them achieve added resonance and reach.

As has been the case in the past, authoritarian-generated digital influence operations need not rely on false information to achieve effect. Russian influence operations have also amplified genuine feelings of gratitude among the Italian population for medical and scientific assistance; one video shows an Italian man replacing an EU flag with a Russian one, accompanied by a sign saying, "Thank you Putin. Thank you, Russia."[60] Such narratives can be circular and cyclical. At times, disinformation narratives from Italy are also directed back into Russia. For instance, Italian-generated anti-NATO narratives surrounding the

Defender Europe 20 military exercise were circulated back into Russia just as they were beginning to fade away in Italy itself.[61]

Go China, Go Italy

As the other dominant player in authoritarian global digital influence operations, and as the institution with perhaps the most at stake in building alternate narratives surrounding the origin of the pandemic, the CCP has engaged in concerted, global action promoting its own narratives and disinformation in the current moment. Some have marked the CCP's current effort to position itself as a responsible global leader as a new phase in China's manipulation of the global information space.[62] Particularly in the context of the coronavirus pandemic, elements of CCP digital influence strategy have mimicked more aggressive, Kremlin-style tactics in the service of promoting conspiracy theories, sowing distrust in institutions, and discrediting democracy.[63]

For instance, a March investigation published by ProPublica revealed over 10,000 fabricated Twitter accounts involved in a coordinated influence campaign, with ties to the Chinese government. Hijacked accounts were found to have pivoted from denigrating Chinese dissidents and discrediting the Hong Kong protests to posting disinformation about the coronavirus outbreak, and frequently linking several of these topics. In this operation, many posts appeared aimed at influencing ethnic Chinese outside China's borders.[64] Such operations sometimes build on past ones, and may overlay each other. In May 2020, Twitter took down a number of accounts linked to Chinese state actors, targeting Chinese-speaking audiences worldwide and apparently building on previous efforts to influence perceptions of the Hong Kong protests and Chinese billionaire Guo Wengui. The Australian Strategic Policy Institute found that the network had pivoted to attempt to influence perceptions on key issues including the U.S. government's response to domestic protest.[65]

The PRC's digital influence operations are not limited to Chinese-language efforts. According to some reports, state-run, English-language media accounts have used major platforms such as Twitter and Facebook to push narratives of western incompetence and Chinese government generosity.[66] As analysis by the Alliance for Securing Democracy points out, during much of March 2020, four of the top ten most-engaged articles on Facebook from China's state media outlets tracked in its proprietary dataset featured content critical of the U.S. response, while the Twitter account for China's embassy in Italy rose to become one of the ten most-engaged accounts within the organization's dataset. This account generally tweeted glowing stories about China's virus response, but Twitter accounts belonging to top Chinese officials have also spread conspiracy theories that raise doubt about the virus' origin and point to the United States as a source. These conspiracy theories, far from being spread by a single actor, were amplified by several other diplomatic accounts as well as Chinese media outlets.[67] Moreover, they appear to have begun circulating through unofficial accounts as early as January 2020.[68]

Few countries have pushed back publicly on these activities, and in fact, there are indications that behind-the-scenes pressure has resulted in some muting their response to these tactics. In April, the *New York Times* reported that European Union officials softened their criticism of China in a report documenting how governments push disinformation about the coronavirus pandemic, although EU officials denied this was the case.[69]

Taiwan, whose effective response to the virus has been somewhat minimized due to China's broad influence over international institutions including the WHO,[70] often serves as the front line for detecting disinformation from PRC entities. In early March, analysts detected a cross-platform disinformation campaign targeting Taiwan, possibly

emanating from Chinese netizens organizing of their own accord, claiming that the Taiwanese government was hiding virus cases, or that bodies of those who passed away were being hidden or burned in secret. Differences in vocabulary, tones, and characters helped distinguish messages generated in the PRC as opposed to Taiwan, even when their origin was intended to be concealed.[71]

In Italy, where the outbreak was early and widespread, the information environment proved a relatively hospitable target for CCP influence operations and narratives—the Five Star Movement has traditionally supported warmer relations with Beijing, while the country was the first major European country to join the Belt and Road Initiative.[72] Among social media praising Chinese health assistance and celebrating closer cooperation, one analysis found that nearly half of the tweets between March 11 and 23 featuring the hashtag #forzaCinaeItalia ("Go China, go Italy") and over a third hashtagged #grazieCina ("thank you China") were bot-originated. Misleading content was also prevalent: Bots also spread a video purporting to show Italian citizens chanting, "Thank you China" from their windows (and later debunked), a video also shared by official Chinese accounts.[73]

Broader PRC narratives have also pushed authoritarian governance as preferable to democracy during the crisis, and have more generally sought to weaken European cohesion and solidarity. A blog post written by the Chinese ambassador to France scolded European critics of the PRC and suggested lessons the world should learn from China's ostensibly more effective authoritarian model.[74] In Europe more broadly, some analysts have raised the concern that a combination of disinformation and PRC health diplomacy, echoed by local proxies on the continent, could pave the way for wider influence in other sectors in the wake of the crisis.[75] More generally, the CCP's more assertive approach to the information space may have repercussions for citizens of autocracies as well as vulnerable and advanced industrialized democracies around the world. Far from being understood as a cautionary tale, it is possible that with enough narrative massaging, China's initial suppression of information and clampdown on whistleblowers may provide a model for others, with implications for international cooperation on pandemic response—authoritarian leaders may be less likely to share information with other countries, permit observation from outside experts, or collaborate internationally.[76] Such ripple effects would have long-lasting implications for governance as well as public health.

While there is not sufficient space in this article to address the full scope of CCP aims and tactics in the broader information ecosystem, there are early signs that a greater public acceptance of health surveillance may lead to opportunities for the Chinese party-state to extend its surveillance capabilities at home and abroad. Partnerships currently being put in place, in a variety of localities around the world[77] may aid the collection and processing of vast amounts of data, something analysts have identified as a party-state priority.[78] Moreover, China's longstanding efforts to harness elements of the information space—including platforms, influencers, and other nodes of the broader ecosystem—may pay dividends in the current environment. Statements from pop stars and other influencers praising China's response[79] demonstrate that the party-state's robust and carefully built propaganda apparatus, including documentaries, entertainment, and other elements, can be brought to bear on the current moment.[80]

Convergence and Amplification

The heightened chaos and swirl of misinformation surrounding the COVID-19 crisis has presented wider opportunities for authoritarian regimes to exacerbate divisions as well as amplify each other when strategically advantageous. For instance, there

A charter flight carrying a 9-member Chinese aid team and 31 tons of medical supplies arrived in Rome, March 12, 2020. (People's Daily, 13 March 2020)

are indications that digital influence operations surrounding the virus have served to further heighten tensions, and provide opportunities for attacks, among Gulf adversaries.[81]

At the same time, the efforts of Beijing, the Kremlin, Tehran, and others can complement each other even when specific narratives diverge, as many have an interest in weakening democratic cohesion.[82] In spreading a particular conspiracy theory regarding the purported U.S. origin of the virus, Chinese officials have relied upon and retweeted narratives put forth by organizations, some of which have reportedly received Russian money, that already have an audience in western countries. These official account amplifications have then found themselves echoed in the wider disinformation echo chamber that exists in the United States and across the world.[83]

According to analysis by the Alliance for Securing Democracy, since November 2019 three of the top five outlets most retweeted by Beijing-linked accounts were funded by the Russian or Iranian governments, while individuals associated with Russian government-funded outlets or pro-Kremlin websites were among the 100 most retweeted accounts by Chinese accounts in their proprietary dataset.[84] Thus, while some analysts have stressed differences in the Russian and Chinese approaches,[85] it is possible that the current pandemic may provide even greater opportunities

for collaboration and amplification, relying on the global disinformation echo chamber for maximum reach, than existed in the past.

Some may ask if opportunities for collaboration and amplification necessarily lead to "impact." The question of impact is a tricky one, since it can be defined in numerous ways. Does only evidence of a real-world outcome that can be directly attributed to an influence operation count as impact? What about less quantifiable shifts in the nature and structure of the global information environment? The truth is, metrics for measuring the "impact" of digital influence operations are still evolving. Researchers can track how far certain operations spread, into which networks, and so on, using social network analysis and other methods. But we are still developing ways to understand how authoritarian digital influence operations may target and influence perceptions around specific narratives in certain countries, and specialized polling methodologies have not yet been put to this purpose.[86] Until more granularity in attribution emerges, one can point to correlations; for instance, in Serbia, where China has been blanketing the country with information and other types of influence operations, four out of ten Serbians think China is the biggest donor to the country (it is in fact the EU).[87]

Getting to a Resilient Democratic Response

While the issues laid out here have pressing and direct ramifications for national security and great power competition, traditional security-based frameworks, processes, and "weapons" do not easily stretch to accommodate these challenges. Because these operations strike at the heart of democratic societies, societies themselves must be part of the solution—in ways that go beyond typical conceptions of national security, yet also protect key civil and political rights.

This can be challenging from a policy perspective. Issues relating to democracy, authoritarianism, and the quality of the media environment have typically been relegated to a different basket of concerns in the foreign policy context than those concerning, for instance, cyber threats. While the former is typically addressed through support for freedom of expression, key political rights, and independent media in other countries, the latter is typically considered a defense or homeland security issue. Authoritarian digital influence operations do not fall neatly into any of these categories, and at times touch multiple dimensions across foreign and domestic policy.

But addressing authoritarian digital influence operations outside the traditional national security lens is not straightforward. In the current policy discourse, this may devolve to putting the onus primarily on the technology platforms to take care of the problem. Yet tech platform action, while necessary, cannot form the sum total of the response. Certainly, the tech platforms have become more proactive in identifying and taking down coordinated inauthentic behavior stemming from state or state-linked actors: Much of the research and takedown action cited in this article stems from company action. The current coronavirus pandemic has further incentivized companies to get tougher on conspiracy theories and other forms of mis- and disinformation that may have public health ramifications.[88]

That said, there is widespread sentiment that technology companies must do more to prevent authoritarian digital influence operations in particular, while at the same time not focusing unduly on content-based remedies that may inadvertently chill speech and comport with authoritarian aims. The European Commission Vice President overseeing the EU's Code of Practice on Disinformation—self-regulation under which platforms have committed to deleting fake accounts and regularly

reporting on manipulation—has urged companies to do more than they are currently.[89] At the same time, civil society organizations have raised concerns that making platforms more broadly liable for speech they host may have a chilling effect on expression and could contribute to a splintered global internet.

Some solutions propose bypassing the sticky issue of content moderation in favor of more seriously interrogating the business model underlying the major platforms, which—in the name of data collection and attention—may provide fertile ground for such influence campaigns. Others suggest ways to alter the design of platforms to encourage more credible content to rise to the fore. Karen Kornbluh and Ellen Goodman have suggested, for instance, user interface defaults that favor transparency, through better labeling; user-customized algorithmic recommendations and ways to track content complaints; and design solutions that introduce friction into the system (say, by limiting forwarding on messages, or encouraging users to read articles before sharing). All of this would make it harder for disinformation to thrive (and, conversely, easier for users to engage constructively). These changes, they argue, would need to be accompanied by privacy laws updated for the digital age—making it harder for all sorts of actors to gain access to individuals' data and target them for influence operations—and national security information sharing between and with the platforms on authoritarian digital influence operations and other actions targeting democratic integrity.[90] These and other innovative suggestions point to a future in which tech companies can—if they wish—build resilience into the design and functioning of their platforms.

Because regulatory or other solutions to the platform issue seem overly complex and burdensome, many turn to the idea of "digital literacy" as the answer to building a resilient response to authoritarian digital influence operations. Yet, just as the entire onus cannot be laid at the feet of the technology companies, it also cannot be the burden of the individual information consumer to simply become more literate and effective in sorting out authentic from inauthentic behavior. While the initial flurry of activity around disinformation and other digital influence operations focused on fact-checking, this is increasingly seen as just one part of a multilayered solution rather than an effective fix on its own. For one thing, sometimes—as highlighted in examples here—the information amplified in digital influence operations is actually true; it is simply being presented without context, or twisted in such a way to fit overarching narratives. Moreover, fact-checking does little against broader narratives and coordinated campaigns of inauthentic activity that are then picked up and amplified by organic networks. Even the most ambitious fact-checking campaign finds it difficult to travel as far and as fast as the original piece of information. Fact-checking also does not address the psychological drivers behind the "demand" for disinformation on the part of news consumers: If individuals are invested in a particular political narrative, they may be more likely to reject corrective information and rationalize their pre-existing beliefs.[91]

Not all digital literacy efforts are the same, and there have been pioneering efforts that deliberately seek to inoculate news consumers against authoritarian disinformation in particular—for instance, in Ukraine.[92] As these efforts are rolled out more broadly, there will need to be stronger efforts to learn relevant lessons from pilots and scale up in a way that is effective. But the learning curve on digital literacy remains steep, even as it is frequently mentioned as a kind of cure-all for a variety of ills related to mis- and disinformation.

The gatekeepers of the information ecosystem—traditional and digital media companies, editors, curators, and others—have their own role to play in mitigating the scope and scale of

authoritarian digital influence efforts. Some have recommended a blueprint for action on norm building across information-related industries, applied to both consumers and producers, with a particular focus on the labeling of authoritarian state-linked media.[93] Certainly, more widespread recognition of the part played by specific authoritarian media outlets in the broader authoritarian digital influence spectrum would help inoculate societies to their divisive aims, and might limit their reach. Action to clearly label outward-facing digital influence operations that utilize platforms banned at home by authoritarian countries might also help distinguish such content in a helpful way for information consumers.

Because the challenge has been so complex, democracies have been slow to devise comprehensive responses to the challenge. They have also been slow to more fully embrace as part of the solution key non-governmental aspects of resilience, including elements of the media, technology, cultural, academic, and other sectors. Yet, precisely because these challenges are cross-cutting and interdisciplinary, the response to them must be similarly multidimensional. On these issues, governments may lead, but they must also look for leadership to these institutions, that—even absent formal public-private partnerships—must take action on their own, and preferably together. Although authoritarian digital influence operations as addressed here are distinct from cybersecurity threats, this aspect of the necessary response is similar: These elements of civil society form the fabric of the "critical infrastructure" in the information space, and thus must play an active role in its protection. Moreover, these efforts would ideally go beyond voluntary piecemeal initiatives to encompass collective vision and action, on norms as well as specific measures. The ideas presented here represent an attempt to broaden the aperture for national security thinking on these ideas.

As the trends leading up to the current information crisis demonstrate, the need to address acute and persistent challenges emanating from the information space will form a distinct feature of the international security environment for the foreseeable future. It is imperative that democratic governments and civil society together lead a robust and multi-layered counter-strategy, preferably one firmly premised upon democratic values. In the meantime, authoritarian regimes will continue to press their advantage, whether democracies muster an effective response or not. PRISM

Endnotes

[1] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It.* (Santa Monica: RAND Corporation, 2016). Available at https://www.rand.org/pubs/perspectives/PE198.html.

[2] Maksymilian Czuperski, John Herbst, Eliot Higgins, Frederic Hof, and Ben Nimmo, *Distract, Deceive, Destroy: Putin at War in Syria*. (Washington, DC: Atlantic Council, April 2016). Available at https://publications.atlanticcouncil.org/distract-deceive-destroy/assets/download/ddd-report.pdf.

[3] Seva Gunitsky, "The Great Online Convergence: Digital Authoritarianism Comes to Democracies," *War on the Rocks*, Feb. 19, 2020. Available at https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/.

[4] *Report Of The Select Committee On Intelligence, United States Senate, On Russian Active Measures: Campaigns And Interference In The 2016 U.S. Election, Volume 2: Russia's Use Of Social Media With Additional Views.* Available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[5] Dean Jackson, "Issue Brief: How Disinformation Impacts Politics and Publics," International Forum for Democratic Studies, May 29, 2018. Available at https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/.

[6] Javier Lesaca, "Why did Russian social media swarm the digital conversation about Catalan independence?" *The Washington Post*, Nov. 22, 2017. Available at https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/.

[7] Jessica Brandt, "Beijing's Viral Disinformation Activities," Power 3.0, April 2, 2020. Available at https://www.power3point0.org/2020/04/02/beijings-viral-disinformation-activities/.

[8] Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation*. Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda. Available at https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

[9] Shanthi Kalathil, *Beyond the Great Firewall: How China Became a Global Information Power.* (Washington, DC: Center for International Media Assistance, March 2017). Available at https://www.cima.ned.org/resource/beyond-great-firewall-china-became-global-information-power/.

[10] Kim Zetter and Joseph Cox, "Here Is the Technical Report Suggesting Saudi Arabia's Prince Hacked Jeff Bezos' Phone," *Vice*, Jan. 22, 2020. Available at https://www.vice.com/en_us/article/v74v34/saudi-arabia-hacked-jeff-bezos-phone-technical-report.

[11] Shanthi Kalathil, "Transparency and Volatility: International Relations in the Information Age," in Shanthi Kalathil, ed., *Diplomacy, Development and Security in the Information Age* (Washington, DC: Institute for the Study of Diplomacy, Georgetown University, 2011) Available at https://cpb-us-e1.wpmucdn.com/blogs.roosevelt.edu/dist/a/14/files/2010/09/Diplomacy_Development_Security_in_the_Information_Age-1.pdf.

[12] Anya Schiffrin, ed., *In the Service of Power: Media Capture and the Threat to Democracy.* (Washington, DC: Center for International Media Assistance, 2017). Available at https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/1174/cima-media-capture-book-f.pdf.

[13] Christopher Walker, Alexis de Tocqueville Annual Lecture, Institute for Political Studies, Catholic University of Portugal, March 5, 2020.

[14] Edward Lucas, *Firming Up Democracy's Soft Underbelly: Authoritarian Influence and Media Vulnerability* (Washington, D.C.: International Forum for Democratic Studies, February 2020). Available at https://www.ned.org/sharp-power-democratic-resilience-series-firming-up-democracys-soft-underbelly/.

[15] Karen Kornbluh, Ellen Goodman, and Eli Wiener, *Safeguarding Democracy Against Disinformation* (Washington, DC: The German Marshall Fund of the United States, 2020). Available at http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation.

[16] Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China* (Lanham, Md: Rowman & Littlefield, 2008).

[17] Mark Bergen, "YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant," Bloomberg, April 2, 2019. Available at https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant.

[18] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* (New York: PublicAffairs, 2019).

[19] Nathalie Marechal and Ellery Roberts Biddle, *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge.* (Washington, DC: Ranking Digital Rights, New America Foundation, March 2020). Avaiable at https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/.

[20] Emma Woollacott, "Social Media Platforms Easy To Manipulate, NATO Advisers Find," Forbes, Dec. 6, 2019. Available at https://www.forbes.com/sites/emmawoollacott/2019/12/06/youtube-is-easiest-platform-to-manipulate-nato-advisers-find/#4aeba8fc3255.

[21] Ronald Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media." *Journal of Democracy* 30, no. 1 (2019): 25–39. Available at https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/.

[22] Bradshaw and Howard, *Global Disinformation Disorder.*

[23] Available at https://freedomhouse.org/explore-the-map?type=fiw&year=2020.

[24] Bradshaw and Howard, *Global Disinformation Order.*

[25] Dean Jackson, "Issue Brief: The 'Demand Side' of the Disinformation Crisis," International Forum for Democratic Studies, Aug. 2, 2018. Available at https://www.ned.org/issue-brief-the-demand-side-of-the-disinformation-crisis/.

[26] Samuel Woolley and Katie Joseff, *Demand for Deceit: How the Way We Think Drives Disinformation*. (Washington, DC: International Forum for Democratic Studies, January 2020). Available at https://www.ned.org/wp-content/uploads/2020/01/Demand-for-Deceit.pdf.

[27] Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality.* (New York: Public Affairs, 2019).

[28] Tim Starks, Laurens Cerulus, and Mark Scott, "Russia's manipulation of Twitter was far vaster than believed," *Politico*, June 5, 2019. Available at https://www.politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543.

[29] Renée DiResta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019.* (Stanford: Internet Observatory Cyber Policy Center, 2019). Available at https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf.

[30] H. Akin Unver, "Russia Has Won the Information War in Turkey," Foreign Policy, April 21, 2019. Available at https://foreignpolicy.com/2019/04/21/russia-has-won-the-information-war-in-turkey-rt-sputnik-putin-erdogan-disinformation/.

[31] Shelby Grossman, Daniel Bush, and Renée DiResta, *Evidence of Russia-Linked Influence Operations in Africa* (Stanford: Stanford Internet Observatory Cyber Policy Center, 2019). Available at https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

[32] Emerson T. Brooking and Suzanne Kianpour, *Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century* (Washington, D.C.: Atlantic Council, 2020). Available at https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.

[33] Bradshaw and Howard, *Global Disinformation Order.*

[34] "#TrollTracker: An Iranian Messaging Laundromat," DFRLab, Aug. 29, 2018. Available at https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193.

[35] Alice Revelli and Lee Foster, "'Distinguished Impersonator' Information Operation That Previously Impersonated U.S. Politicians and Journalists on Social Media Leverages Fabricated U.S. Liberal Personas to Promote Iranian Interests," FireEye Threat Research, Feb. 12, 2020. Available at https://www.fireeye.com/blog/threat-research/2020/02/information-operations-fabricated-personas-to-promote-iranian-interests.html.

[36] Bradshaw and Howard, *Global Disinformation Order.*

[37] Katie Benner, Mark Mazzetti, Ben Hubbard and Mike Isaac, "Saudis' Image Makers: A Troll Army and a Twitter Insider," *The New York Times*, Oct. 20, 2018. Available at https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html.

[38] Renée DiResta, Shelby Grossman, K.H., and Carly Miller, *Analysis of Twitter Takedown of State-Backed Operation Attributed to Saudi Arabian Digital Marketing Firm Smaat* (Stanford: Internet Observatory Cyber Policy Center, 2019). Available at https://cyber.fsi.stanford.edu/io/news/smaat-twitter-takedown.

[39] Leena Khalil, "Inside the Middle East's epic online propaganda war," Wired, Sept. 29, 2019. Available at https://wired.me/technology/privacy/inside-the-middle-easts-epic-online-propaganda-war/.

[40] Sarah Cook, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence Since 2017.* (New York: Freedom House, 2020). Available at https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.

[41] Kalathil, *Beyond the Great Firewall.*

[42] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas, *Mapping China's Technology Giants.* Australian Strategic Policy Institute, Report No. 15, 2019. Available at https://www.aspi.org.au/index.php/report/mapping-chinas-tech-giants.

[43] Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," Foreign Policy, June 26, 2019. Available at https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

[44] Tom Uren, Elise Thomas and Jacob Wallis, *Tweeting through the Great Firewall: Preliminary analysis of PRC-linked information operations against the Hong Kong protest.* Australian Strategic Policy Institute, Report No. 25, 2019. Available at https://www.aspi.org.au/report/tweeting-through-great-firewall.

[45] "China is using Facebook to build a huge audience around the world," *The Economist*, April 20th, 2019. Available at https://www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world?cid1=cust/ednew/n/bl/n/2019/04/17n/owned/n/n/nwl/n/n/NA/228993/n.

[46] *2019 Ranking Digital Rights Corporate Accountability Index*. Available at https://rankingdigitalrights.org/index2019/.

[47] Lily Kuo, "TikTok 'makeup tutorial' goes viral with call to action on China's treatment of Uighurs," *The Guardian*, Nov. 26, 2019. Available at https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs.

[48] Alex Hern, "Revealed: how TikTok censors videos that do not please Beijing," The Guardian, Sept. 25, 2019. Available at https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

[49] Michael Walsh, Stephen Dziedzic, and Jason Fang, "Why are Australian politicians intensifying their presence on Chinese social media platforms?" Australian Broadcasting Corporation, April 4, 2019. Available at https://mobile.abc.net.au/news/2019-04-04/why-are-australian-politicians-jumping-on-chinese-social-media/10966152?pfmredir=sm.

[50] See, e.g., numerous articles analyzing WeChat censorship by Canada-based Citizen Lab. Available at https://citizenlab.ca/tag/wechat/.

[51] Christopher Walker, Shanthi Kalathil, and Jessica Ludwig. "The Cutting Edge of Sharp Power." *Journal of Democracy* 31, no. 1 (2020): 124–37.

[52] Woolley and Joseff, *Demand for Deceit*.

[53] Jonathan Bright, Hubert Au, Hannah Bailey et al, "COVID-19 Series Coronavirus Coverage by State-Backed English-Language News Sources: Understanding Chinese, Iranian, Russian and Turkish Government Media," Oxford Internet Institute, April 8, 2020. Available at https://comprop.oii.ox.ac.uk/research/state-media-coronavirus/.

[54] "EEAS Special Report: Disinformation on the coronavirus – short assessment of the information environment," EUvsDisinfo, March 19, 2020. Available at https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/.

[55] Max Fisher, "Why Coronavirus Conspiracy Theories Flourish. And Why It Matters," *The New York Times*, April 8, 2020. Available at https://www.nytimes.com/2020/04/08/world/europe/coronavirus-conspiracy-theories.html#click=https://t.co/heCj4k07Sc.

[56] Robin Emmott, "Russia deploying coronavirus disinformation to sow panic in West, EU document says," Reuters, March 18. 2020. Available at https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F.

[57] "EEAS Special Report," March 19, 2020.

[58] Patrick Tucker, "Russia Pushing Coronavirus Lies As Part of Anti-NATO Influence Ops in Europe," Defense One, March 26, 2020. Available at https://www.defenseone.com/technology/2020/03/russia-pushing-coronavirus-lies-part-anti-nato-influence-ops-europe/164140/.

[59] "Russia exploits Italian coronavirus outbreak to expand its influence," DFR Lab, March 30, 2020. Available at https://medium.com/dfrlab/russia-exploits-italian-coronavirus-outbreak-to-expand-its-influence-6453090d3a98.

[60] Natalia Antelava and Jacopo Iacoboni, "The influence operation behind Russia's coronavirus aid to Italy," Coda Story, April 2, 2020. Available at https://www.codastory.com/disinformation/soft-power/russia-coronavirus-aid-italy/.

[61] "Italian anti-NATO coronavirus narrative recycled in Russia," DFR Lab, March 23, 2020. Available at https://medium.com/dfrlab/italian-anti-nato-coronavirus-narrative-recycled-in-russia-46f14537c25a.

[62] David Shullman, "How China is Exploiting the Pandemic to Export Authoritarianism," War on the Rocks, March 31, 2020. Available at https://warontherocks.com/2020/03/how-china-is-exploiting-the-pandemic-to-export-authoritarianism/.

[63] Jessica Brandt and Bret Schaefer, "Five Things to Know About Beijing's Disinformation Approach," Alliance for Securing Democracy, March 30, 2020. Available at https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.

[64] Jeff Kao and Mia Shuang Li, "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus," ProPublica, March 26, 2020. Available at https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus.

[65] Jake Wallis, Tom Uren, Elise Thomas et al, *Retweeting Through the Great Firewall: A Persistent and Undeterred Threat Actor.* Australian Strategic Policy Institute, Policy Brief/Report No. 33, 2020. Available at https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_1.pdf?ZzW5dlyqlOOgG5m9oHj9DWsjgtXD6TCA.

[66] Jane Lytvynenko "Chinese Propaganda Is Trying To Paint The Country As A Leader In Coronavirus Response," Buzzfeed, March 30, 2020. https://www.buzzfeednews.com/article/janelytvynenko/chinese-state-media-coronavirus.

[67] Jessica Brandt, "Beijing's Viral Disinformation Activities," Power 3.0, April 2, 2020. Available at https://www.power3point0.org/2020/04/02/beijings-viral-disinformation-activities/.

[68] Vanessa Molter and Graham Webster, "Coronavirus Conspiracy Claims: What's Behind a Chinese Diplomat's COVID-19 Misdirection," Stanford Cyber Policy Center, March 31, 2020. Available at https://cyber.fsi.stanford.edu/news/china-covid19-origin-narrative.

[69] Matt Apuzzo, "Pressured by China, E.U. Softens Report on Covid-19 Disinformation" *The New York Times*, April 24, 2020. Available at https://www.nytimes.com/2020/04/24/world/europe/disinformation-china-eu-coronavirus.html.

[70] Hal Brands, "China's Global Influence Operation Goes Way Beyond the WHO," Bloomberg, March 31, 2020. Available at https://www.bloomberg.com/opinion/articles/2020-03-31/china-s-influence-operation-goes-beyond-who-taiwan-and-covid-19?srnd=opinion.

[71] Nick Monaco, "No Rest for the Sick: Coronavirus Disinformation from Chinese Users Targets Taiwan," Digital Intelligence Lab, March 5, 2020. Available at https://medium.com/digintel/china-coronavirus-disinfo-targets-taiwan-2490d99ce6a9.

[72] Mattia Ferraresi, "China Isn't Helping Italy. It's Waging Information Warfare," Foreign Policy, March 31, 2020. Available at https://foreignpolicy.com/2020/03/31/china-isnt-helping-italy-its-waging-information-warfare/.

[73] Francesco Bechis and Gabriele Carrer, "How China Unleashed Twitter Bots To Spread COVID-19 Propaganda in Italy," Formiche, March 31, 2020. Available at https://formiche.net/2020/03/china-unleashed-twitter-bots-covid19-propaganda-italy/.

[74] Available at http://www.amb-chine.fr/fra/zfzj/t1762848.htm?utm_source=Disinformation+Matters&utm_campaign=a2dc1afaca-EMAIL_CAMPAIGN_2020_04_01_12_17&utm_medium=email&utm_term=0_610841f0e2-a2dc1afaca-255848637.

[75] Naja Bentzen, "COVID-19 foreign influence campaigns: Europe and the global battle of narratives," European Parliamentary Research Service, April 2020. Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS_BRI(2020)649367_EN.pdf.

[76] Shullman, "How China is Exploiting the Pandemic."

[77] Morgan Meaker, "Marseille's fight against AI surveillance," Coda Story, March 26, 2020. Available at https://www.codastory.com/authoritarian-tech/ai-surveillance-france-crime/.

[78] Samantha Hoffman, *Engineering global consent: The Chinese Communist Party's data-driven power expansion*, Australian Strategic Policy Institute, October 14, 2019. Available at https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[79] Jiayun Feng, "'I want no smoke with the Chinese': Cardi B wins fans in China with coronavirus rants," supchina, March 26, 2020. Available at https://supchina.com/2020/03/26/i-want-no-smoke-with-the-chinese-cardi-b-wins-fans-in-china-with-coronavirus-rants/.

[80] Kalathil, *Beyond the Great Firewall*.

[81] Ryan Grace, "COVID-19 prompts the spread of disinformation across MENA," Middle East Institute, March 20, 2020. Available at https://www.mei.edu/publications/covid-19-prompts-spread-disinformation-across-mena.

[82] Tony Romm, "Facebook disables Russian and Iranian efforts to manipulate users, raising new 2020 election fears," The Washington Post, Feb. 12, 2020. Available at https://www.washingtonpost.com/technology/2020/02/12/facebook-russia-iran-myanmar-disinformation/.

[83] Julian E. Barnes, Matthew Rosenberg, and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," The New York Times, March 28, 2020. Available at https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html.

[84] Brandt, "Beijing's Viral Disinformation Activities."

[85] Jean-Baptiste Jeangène Vilmer and Paul Charon, "Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare," War on the Rocks, January 21, 2020. Available at https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/.

[86] Christopher Walker, Shanthi Kalathil and Jessica Ludwig, "Forget Hearts and Minds," *Foreign Policy*, Sept. 14, 2018. Available at https://foreignpolicy.com/2018/09/14/forget-hearts-and-minds-sharp-power/.

[87] Mentioned in a tweet by Mikko Huotari, data attributed to RFE/RL. Available at https://twitter.com/m_huotari/status/1271816348486832128.

[88] Leo Kelion, "Coronavirus: YouTube tightens rules after David Icke 5G interview," BBC, April 7, 2020. Available at https://www.bbc.com/news/technology-52198946.

[89] Florian Eder, "Věra Jourová: Platforms 'need to open up' algorithms to deal with disinformation," Politico, Dec. 6, 2019. Available at https://www.politico.eu/article/vera-jourova-platforms-need-to-open-up-algorithms-to-deal-with-disinformation/.

[90] Karen Kornbluh, Ellen Goodman, and Eli Wiener, *Safeguarding Digital Democracy: Digital Innovation and Democracy Initiative Roadmap* (Washington, D.C.: The German Marshall Fund of the U.S., March 2020). Available at http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation.

[91] Woolley and Joseff, *Demand for Deceit*.

[92] For instance, see IREX's "Learn to Discern" media literacy programs: https://www.irex.org/project/learn-discern-l2d-media-literacy-training.

[93] Lucas, *Firming Up the Soft Underbelly*.