The specter of Chinese interference: examining Beijing's inroads into India's digital spaces and political activity

Sukumar, A.M.; Deo, A.; Ohlin, D.; Hollis, D.B.

5

The Specter of Chinese Interference

Examining Beijing's Inroads into India's Digital Spaces and Political Activity

Arun Mohan Sukumar and Akhil Deo

I. Introduction

Banner events tend to steer scholarship and policy prescriptions. Thus, Russian efforts to manipulate the outcome of the 2016 U.S. presidential elections have dominated the discourse on election interference by foreign powers. "The Russian playbook," as it was termed by a top elected official of the American national security apparatus,[1] may well be adopted by other nation-states in the months to come. However, the impact of similar interventions—measured both in terms of their intended outcomes and the degrading of the integrity of digital infrastructure—will depend on a number of factors. The strategic and economic context in which foreign election interference occurs through digital platforms is naturally important. Traditional geopolitical rivalries, such as the one between the United States and Russia, have inspired online disinformation campaigns across regions, especially in the Middle East.[2] But the record of many of these interventions, to quote one forensic analysis, is "equivocal."[3] Governments, social media platforms, digital news outlets, fact-checking organizations, and research institutions are today more cognizant than ever of disinformation campaigns, making sustained malicious activity almost impossible to go undetected. That Russia's own attempt at influencing the 2018 U.S. midterm elections were purportedly less successful than its intervention two years previously attests to this reality.[4]

Equally important are the personnel and technical resources a foreign actor has invested in the craft of "old-world" espionage—identifying issues, communities, or constituencies most pliable to digital manipulation. Few states can bring to bear the sustained resources, attention, and expertise in orchestrating disinformation campaigns as Russia has historically done. China, however, is one such state. Its rising

[1] Julian E. Barnes, *Russians Tried, but Were Unable to Compromise Midterm Elections, U.S. Says*, N.Y. Times (Dec. 21, 2018).

[2] Nabih Bulos, *Coronavirus becomes a Weapon of Disinformation in Middle East Battle for Influence*, L.A. Times (Apr. 8, 2020); *Inside Saudi Arabia's Disinformation Campaign*, NPR (Aug. 10, 2019).

[3] Gabrielle Lim et al., *Burned After Reading: Endless Mayfly's Ephemeral Disinformation Campaign* (The Citizen Lab, May 14, 2019), *at* https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/.

[4] Barnes, *supra* note 1.

Arun Mohan Sukumar and Akhil Deo, *The Specter of Chinese Interference* In: *Defending Democracies*. Edited by Duncan B. Hollis and Jens David Ohlin, Oxford University Press (2021).
DOI: 10.1093/oso/9780197556979.003.0006

global economic and political clout, accompanied by the explosive growth of its technology companies, offers China both the tools and the playgrounds to effect electoral interference in foreign jurisdictions. In fact, as this chapter argues, China's success in manipulating elections may leave Russia far behind, given the many levers it has to channel propaganda and the relative lack of attention paid to disinformation in Chinese digital platforms over, say, a Facebook, WhatsApp, or Twitter.

This chapter highlights the prospects for election interference by China in the world's largest democracy, India. It charts the pathways by which China could mount a sophisticated disinformation campaign targeting India's political processes and outlines the growing incentives for Beijing to engage in such operations. Concerns around Chinese influence operations against India are not hypothetical: in 2020, the Indian government banned 224 Chinese mobile apps, including TikTok, WeChat, and Alipay, citing national security risks. This extraordinary measure, the government announced, was motivated by reports of apps "stealing and surreptitiously transmitting users' data in an unauthorized manner" outside India, and the use of such data for "mining and profiling by elements hostile to the national security and defence of India."[5] That the ban was imposed in the aftermath of a violent confrontation in the summer of 2020 between Chinese and Indian armed forces along their disputed Himalayan border is significant. While its duration is unclear, the ban reflects the Indian security establishment's heightened concern that China may weaponize its highly popular digital platforms towards cyber attacks and influence operations against an increasingly adversarial neighbor. To be sure, we do not offer a smoking gun to highlight China's complicity in, or planning of, digital interference in an ongoing or past election campaign in India. Rather, we hold up recent instances where state-based actors appear emboldened to facilitate disinformation campaigns. The objective of this chapter is to present a framework by which China's cyber operations to influence the outcome of elections—not only in India but also in other markets where Chinese companies have a growing presence—can be studied.

To the authors' best knowledge, there currently exists no systematic assessment of Chinese election interference in India: indeed, at the time of writing, there are few scholarly assessments of Chinese influence operations, even including documented ones in Hong Kong SAR and Taiwan.[6] As a 2019 study by the Oxford Internet Institute concluded, "[until recently,] China rarely used social media to manipulate public opinion in other countries."[7] As recently as 2018, Western intelligence agencies believed China would extend the same "techniques developed for domestic control [such as censorship and promotion of ideological propaganda] to foreign audiences."[8] That is evidently changing, and this chapter attempts to outline the "whys" and "hows"

[5] *Ministry of Electronics and IT—Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order*, Press Information Bureau (Sep. 02, 2020).

[6] *Taiwan Election: Disinformation as a Partisan Issue* (Stanford Cyber Policy Center, Jan. 21, 2020), *at* https://cyber.fsi.stanford.edu/io/news/taiwan-disinformation-partisan-issue.

[7] Samantha Bradshaw & Philip N. Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Working Paper 2019.3 2 (Oxford Internet Institute Project on Computational Propaganda, 2019).

[8] *Who Said What? The Security Challenges of Modern Disinformation*, World Watch: Expert Notes Series 78 (Canadian Security Intelligence Services, Pub. No. 2016-12-05, 2018).

of Chinese influence operations targeted at political processes, highlighting India as a case study.

Our chapter is divided into four segments. The first section highlights the evolution of China's strategy, broadly defined, toward disinformation and influence operations in the digital age. The second fleshes out the contours of India's own maturing digital economy and the steady online migration of political activity, which we argue renders its democratic processes susceptible to election interference. The third section reviews extent practices of Chinese technology companies—which have built a vast user/ client network in India—with regards to the management and security of data, as well as their handling of malicious and false content. And finally, we hold up a number of conceivable incentives for China to intervene in India's electoral processes, both at the federal and at the state level.

Before doing so, however, a few caveats are in order. This chapter does not survey the security of India's election infrastructure such as voter rolls and electronic voting machines or attendant computer systems used in the polling process. In 2019, ahead of the country's general election, the Election Commission of India issued a series of detailed cybersecurity guidelines, which present vectors of vulnerability in India's digital networks.[9] Those vectors are susceptible to exploitation by China given the expansive role of Chinese companies in India's telecommunications infrastructure, handheld device market, and apps ecosystem. A detailed review of those vulnerabilities are in order, but this chapter does not undertake it; rather, it highlights other patent opportunities India's "digital public sphere" presents to China in order to interfere in the country's democratic processes.

II. The Evolution of China's Approach to Disinformation

Although a detailed history of China's evolving approach on influence operations is outside the scope of this chapter, it is important to recognize that China has long considered information a battleground for power. Thus, control over discourse and narratives at home has always been a core interest for the Communist Party.[10] Over the past decade, China's efforts have expanded to include discourse and narratives abroad.

Its efforts to influence global perception have taken on three distinct forms. The first is through what Chinese strategists call "borrowing the boat to sail into the ocean"—or paid inserts into foreign media publications.[11] Reports indicate, for instance, that a *China Daily* supplement is published in major newspapers across at least

[9] Election Commission of India, *Cyber Security General Guidelines for General Elections* (July 18, 2019), *at* https://eci.gov.in/files/file/10349-cyber-security-general-guidelines-for-general-election-2019/.

[10] *See generally* David Shambaugh, *China's Propaganda System: Institutions, Processes and Efficacy*, 57 China J. 25–58 (2007); Wu Xuecan, *Turning Everyone into a Censor: The Chinese Communist Party's All-Directional Control over the Media* (U.S.-China Economic and Security Review Commission, 2001); Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* (U.S. Army War College Strategic Studies Institute, 2001).

[11] Sam Geal & Robert Soutar, *Chinese Media and Latin America: "Borrowing a Boat" to Set Sail* (Jamestown Foundation, July 10, 2018), *at* https://jamestown.org/program/chinese-media-and-latin-america-borrowing-a-boat-to-set-sail/.

thirty countries.[12] The *Financial Times* has similarly reported China Global Television Network provides free content to nearly 1,700 media organizations around the world.[13] The second is through "Confucius Institutes," which are cultural and education organizations that are often tied to and fund universities abroad. Multiple reports have documented the opaque nature of this funding, as well as the institutes' censorship of conversations around politically sensitive issues like Taiwan and Tibet.[14] In 2018, the U.S. Congress enacted legislation prohibiting the use of Department of Defense funds for Chinese language training by Confucius Institutes.[15] The measure prompted many universities to sever ties with these institutes.[16] And the third is through diaspora management—a primary function of the United Front Work Department.[17]

These traditional levers of propaganda and influence have gradually evolved over the past two years to include a growing Chinese presence on Western social media platforms, as part of a major effort by the Xi Jinping administration to globalize Chinese media narratives. Xinhua news agency, *Global Times*, CGTN, and *People's Daily*, for example, all have a strong social media presence on Facebook and Twitter. CGTN has nearly 87 million followers,[18] with 20 million followers having been added since 2018 alone.[19] Beijing also employs a vast army of "Internet commentators"—known informally as "50C" party members[20]—to express pro-Party views on Chinese and foreign social media platforms.[21] China's diplomatic establishment and community have similarly made a concerted push onto Twitter, with reports documenting that at least thirty-two Chinese diplomats, embassies, and consulates launched their Twitter accounts in 2019 alone.[22] Unlike Russia, whose disinformation campaigns are intended to sow discord, exploit socioeconomic fault lines, and generally undermine trust in democratic institutions, China's influence efforts on foreign social media platforms have hitherto been largely directed at embellishing the reputation of the Chinese Communist Party (CCP) abroad.

[12] Louisa Lim & Julia Bergin, *Inside China's Audacious Global Propaganda Campaign*, The Guardian (Dec. 7, 2018).

[13] Emily Feng, *China and the World: How Beijing Spreads the Message*, Financial Times (July 12, 2018).

[14] Rachelle Peterson, *Outsourced to China: Confucius Institutes and Soft Power in American Higher Education* 10 (National Association of Scholars, June 2017), *at* https://www.nas.org/reports/outsourced-to-china.

[15] Racqueal Legerwood, *As US Universities Close Confucius Institutes, What's Next?*, Hum. Rts. Watch (Jan. 27, 2020).

[16] Karen Fisher, *Oldest Confucius Institute in U.S. to Close*, The Chronicle of Higher Education (Jan. 22, 2020).

[17] John Fitzgerald, *Loyalty through Links and Control: The Long History of Chinese Diaspora Diplomacy*, The Interpreter (May 11, 2016).

[18] Sarah Cook, *Beijing's Global Megaphone*, Freedom House: Special Report 6 (Jan. 2020), *at* https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.

[19] *Id*.

[20] The phrase "50C" gained popularity based on some assertions that party members were paid 50 US cents per post. Although this has since been disproved, the moniker stuck. *See* Gary King et al., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, 111 Am. Pol'y Sci. Rev. 484, 484–501 (2017).

[21] *Id*.

[22] Zhaoyin Feng, *China and Twitter: The Year China Got Louder on Social Media*, BBC (Dec. 29, 2019).

Recent events suggest, however, that this is beginning to change. Beijing has begun to adopt Russia-style tactics, as it were, in their digital operations. In two related data dumps released in August and September 2019, both Twitter and Facebook banned thousands of fake accounts and pages linked to Chinese actors for attempting to sow discord between pro- and antigovernment protestors in Hong Kong.[23] Many of the accounts linked to this campaign were created as part of an earlier disinformation campaign against Chinese dissident Guao Wengui, as far back as August 2017. Guao Wengui was a popular figure on social media, and Chinese efforts to discredit him were aimed at blunting his criticism ahead of the critical 19th Party Congress in September.[24] The campaign against Guao differs from standard Chinese efforts to influence global narratives. It marked the first time that China-based actors were traced to "inauthentic" behavior on U.S. technology platforms.[25] That Beijing actively engaged in a disinformation campaign is also notable, in contrast to its usual attempts at portraying China or the CCP in a good light.

Another illustration of China's evolving strategy of information "warfare"—and perhaps the only reported instance of China interfering in elections—is its disinformation campaign directed at Taiwan's 2020 presidential race and a related mayoral election earlier in 2018. Although Beijing has long employed different political and media-related measures to interfere in Taiwan's political processes, recent efforts to prevent the re-election of President Tsai Ing-wen by spreading disinformation about her and her policies (and overtly supporting the opposition candidate, who is perceived to be more sympathetic to Beijing), indicate a more aggressive approach.[26] Reports from 2018 suggest, in fact, that the opposition candidate Han Kuo-yu's run for local office was bolstered by inauthentic activity on Facebook and other social media platforms.[27] Although no official sources have attributed these efforts to Beijing, circumstantial evidence pointed to the involvement of the CCP, including the presence of accounts from mainland China,[28] linguistic differences in pages and accounts suspected to have been run by Chinese actors,[29] Twitter's takedown of "troll" accounts and pages related to Hong Kong, and a United Front Work Department conference on "internet influence activities"[30] weeks before the presidential elections. Once again,

[23] *Information Operations Directed at Hong Kong*, Twitter Safety (Aug. 19, 2019), *at* https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html; Nathaniel Gliecher, *Removing Co-Ordinate Inauthentic Behaviour from China*, Facebook Newsroom (Aug. 19, 2020), *at* https://about.fb.com/news/2019/08/removing-cib-china/.

[24] Daniel Wood, Sean McMinn, & Emily Feng, *China Used Twitter to Disrupt Hong Kong Protests, but Efforts Began Years Earlier*, NPR (Sept. 17, 2019).

[25] Emily Stewart, *How China Used Facebook, Twitter, and YouTube to Spread Disinformation about the Hong Kong Protests*, Vox (Aug. 23, 2019).

[26] Brian Hioe, *Fighting Fake News and Disinformation in Taiwan: An Interview with Puma Shen*, New Bloom Magazine (Jan. 6, 2020).

[27] Kathryn Hille, *Taiwan Primaries Highlight Fears over China's Political Influence*, Financial Times (July 17, 2019); Paul Huang, *Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate*, Foreign Pol'y (June 26, 2019).

[28] Connor Fairman, *When Election Interference Fails*, Net Politics (Council on Foreign Relations, Jan. 29, 2020), *at* https://www.cfr.org/blog/when-election-interference-fails.

[29] *Id*.

[30] Raymond Zhong, *Awash in Disinformation before Vote, Taiwan Points Finger at China*, N.Y. Times (Jan. 6, 2020).

these disinformation tactics more closely resembled the Russian campaign targeting the 2016 U.S. presidential elections than traditional Chinese activity.

The most recent incident is China's disinformation campaign, ongoing at the time of writing, around its response to the COVID-19 outbreak in the city of Wuhan and the Hubei province. Beijing has drawn ire from some states and political leaders for its early failures in tackling the outbreak of the coronavirus pandemic in Wuhan.[31] In an effort to deflect attention away from Beijing's purported failures, Zhao Lijian, spokesperson for China's Ministry of Foreign Affairs, tweeted an article titled "COVID-19: More evidence that the virus originated in the US."[32] Sourced from a website known for promoting conspiracy theories, the article suggested that the coronavirus was a bioweapon developed in the United States and subsequently smuggled into Wuhan by the U.S. military.[33] A few weeks later, China's state-run *Global Times* speculated the source of the outbreak to be in Italy.[34] Several official accounts of Chinese embassies around the world subsequently shared either Zhao's tweet or similar assertions of U.S. responsibility in smuggling the virus into China.[35] Most of these accounts were created only in late 2019. Although one analysis of China's COVID-19 social media diplomacy concluded China's state media focused largely on the swiftness of Beijing's response to the crises,[36] the Zhao Lijian incident, and the social media behavior of several other Chinese diplomats and embassies, demonstrates that China is more willing to use its state media outlets to propagate disinformation without concern of being attributed—another departure from standard practice.[37]

III. India's "Marketplace" for Influence Operations

These instances indicate a significant turn in China's efforts to influence global opinions. They also acquire salience as potential pathways for Beijing to influence political processes in states like India. There is a thriving market for disinformation in India, driven by its near-continuous federal and local election cycles, the country's young and internet-savvy demographic that has shown a voracious appetite for social media, and limited institutional oversight and accountability mechanisms over political speech. Taken together, these all make the prospects for a Chinese disinformation campaign highly lucrative. Political parties in India are currently major, if not the

[31] Ishaan Tharoor, *It's Not Just Trump Who's Angry at China*, Washington Post (Apr. 14, 2020).

[32] @zlj517, Twitter (Mar. 13, 2020, 6.32 AM), *at* https://twitter.com/zlj517/status/1238269193427906560?s=20.

[33] Betsy Morris & Robert McMillan, *China Pushes Viral Messages to Shape Coronavirus Narrative*, Wall Street Journal (Apr. 10, 2020).

[34] Chris Chang, *China Now Implying Coronavirus May Have Originated in Italy*, Taiwan News (Mar. 24, 2020).

[35] Mark Scott, *Chinese Diplomacy Ramps Up Social Media Offensive in COVID-19 Info War*, Politico (Apr. 29, 2020).

[36] Vanessa Molter, *Pandemics & Propaganda: How Chinese State Media Shapes Conversations on the Coronavirus* (Stanford Cyber Policy Center, Mar. 19, 2020), *at* https://cyber.fsi.stanford.edu/news/chinese-state-media-shapes-coronavirus-convo.

[37] *See, e.g.*, *"Once Upon a Virus": China Mocks US with Video on Covid-19, Twitter Hits Back*, Hindustan Times (May 1, 2020).

preeminent drivers of disinformation and propaganda.[38] There are plenty of incentives in the form of India's cyclical local and state elections and the bidecadal general elections. The practice of leveraging digital platforms for political campaigns went mainstream during the 2014 Indian General Elections—Prime Minister Narendra Modi's overwhelming electoral success has been partly attributed to his effective social media campaign.[39] Both the Bharatiya Janata Party (BJP) and the Indian National Congress—India's two major national political parties—were reported to have hired digital advertising companies to help bolster their digital presence.[40] It was the 2019 general elections, however, that marked a critical turning point, with candidates, political organizations, and other interest groups in India embracing and harvesting digital platforms for electoral advantage. This shift was largely enabled by rapid advances in India's digital economy in the interim. In 2014, barely 100 million Indians owned smartphones—a number that jumped threefold to 300 million by 2017.[41] The year 2015 also marked the entry of Reliance Jio into India's telecommunications sector, whose initially free and later subsidized offerings contributed to the plummeting of mobile data prices to $0.20 per gigabyte—the cheapest anywhere in the world.[42]

The deployment of digital platforms by all manner of actors to influence the outcome of the 2019 national polls was so extensive it earned the moniker "WhatsApp elections"—named primarily for the outsized role Facebook's messaging app played in spreading legitimate political content as well as patently false information.[43] A significant portion of what platforms now call "inauthentic" political propaganda in India is driven by well-structured, well-funded, and targeted organizations within political outfits—known colloquially as "information technology (IT) cells."[44] Although these organizations possess a staff of their own, their operations are often amplified by loose coalitions of volunteers—upward of a million at a time, according to some reports.[45] This well-defined administrative structure is bolstered by increasingly granular data aggregation practices, some that may rely on harvesting user and behavioral data from social media platforms, but also includes extensive analytics and profiling based on the data gathered from electoral rolls, electricity bills, and ration cards.[46] Party cadres are then placed in charge of hyperlocal content creation strategies that tailor messaging based on the profiles of individuals or communities.

[38] Snigdha Poonam & Samarth Bansal, *Misinformation Is Endangering Indian Elections*, The Atlantic (Apr. 1, 2019).

[39] Derek Willis, *Narendra Modi, the Social Media Politician*, N.Y. Times (Sept. 25, 2014).

[40] Bhavna Vij Arora, *Congress Gears Up for 2014, Awards ad Campaign to JWT with One-Point Agenda to Counter Narendra Modi*, India Today (Sept. 9, 2013); Vidhi Choudhary, Gyan Varma, & Makarand Gadgil, *The Ad Agencies behind BJP's Successful Campaign*, Livemint (Oct. 19, 2014).

[41] Pankaj Mishra, *The Real Revolution in India*, Bloomberg (Apr. 21, 2019).

[42] *India Has Cheapest Mobile Data in the World: Study*, The Hindu (Mar. 6, 2019).

[43] Priyanjana Bengali, *India Had Its first "WhatsApp election." We Have a Million Messages from It*, Colum. Journalism Rev. (Oct. 16, 2019).

[44] *See generally* Ualan Campbell-Smith & Samantha Bradshaw, *Global Cyber Troops Country Profile: India* (Oxford Internet Institute, May 2019), *at* https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf.

[45] Dinesh Narayan & Venkat Ananth, *How the Mobile Phone Is Shaping to Be BJP's Most Important Weapon in Elections*, Economic Times (Aug. 23, 2018).

[46] Shivam Shankar Singh, *How Political Parties Mixed Data Analytics and Social Media for Disinformation Campaigns*, Medianama (Apr. 12, 2019).

Enabling this ecosystem is a growing network of marketing agencies, political consultancies, influencer networks, and analytics platforms. Cambridge Analytica, for instance, was hired by both national political parties in India—the Congress and the BJP.[47] News reports and interviews with current and former campaign management staff for Indian political parties suggest a longer list of such partnerships. A digital marketing firm in New Delhi, OML Logic, for instance, has similarly been hired both by the BJP and the Congress to manage social media content.[48] Such practices go well beyond national parties and include regional outfits. Reports from the southern Indian state of Andhra Pradesh suggest the Telugu Desam Party hired Pramanya Strategy Consulting Private Ltd. to manage digital campaigns.[49] There is limited information about how these firms actually operate and negligible pressure on political parties to be transparent about the type of campaigns they run. (During the 2019 general elections, the Election Commission of India included prohibitions against fake news and rumormongering in its "model code of conduct" for political parties and contesting candidates, but this has had very little discernible effect.[50]) Anecdotal evidence suggests a very similar approach to those employed by Cambridge Analytica during the 2016 American elections. One Delhi-based firm, Obiyan Infotech, boasts on its website, for instance, that it can harvest "quite a few indicators that may help predict whom a voter is inclined to vote for."[51]

That political parties were heavily leveraging both their cadre and third parties to influence India's digital spaces became apparent a month before the general elections in May 2019, when Facebook took down nearly 700 pages and accounts belonging to both the BJP and Congress for "coordinated inauthentic behavior."[52] Around 15 of the pages were managed by Silver Touch, a political consultancy linked to the BJP. Another 678 pages were linked to members of the Congress's IT cell. One of the pages that was taken down, "The Indian Eye," was a pro-BJP page that was integrated into the "Narendra Modi" application, which boasts over 10 million downloads and was promoted as a means for the prime minister to stay "in touch" with ordinary citizens.[53]

IV. Practices of China's Technology Platforms in India

Exacerbating the risk of Chinese influence operations within what is already a manipulable Indian "digital public sphere" is the rapid entry of Chinese content applications

[47] Vidhi Doshi & Annie Gowen, *Whistleblower Claims Cambridge Analytica's Partners in India Worked on Elections, Raising Privacy Fears*, WASHINGTON POST (Mar. 29, 2018).

[48] Anumeha Chaturvedi, *Ahead of General Elections, Parties Tap Social Media Influencers*, ECONOMIC TIMES (Mar. 1, 2019).

[49] *In Google Ad Spend, TDP Is Beating BJP Now*, ECONOMIC TIMES (Apr. 4, 2019).

[50] *EC's Social Media Guidelines May Not Be Enough*, HINDUSTAN TIMES (Mar. 13, 2019).

[51] Obiyan Infotech, *Digital Marketing for Politicians in India: Mantra of Success*, *available at* https://www.obiyaninfotech.com/digital-marketing-for-politician/.

[52] Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior and Spam from India and Pakistan*, FACEBOOK NEWSROOM (Apr. 1, 2019), *at* https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/.

[53] *NaMo App Promotes Fake News Factory "The India Eye" and Users Can't Block It Even If They Want To*, SCROLL (Feb 7, 2019).

in India's digital economy. Consider, for instance, that in 2017, eighteen of the one hundred most downloaded apps on the Indian Google Play store were Chinese.[54] In 2018, this number rose dramatically to forty-four. Chinese applications now cut across various categories, but a significant number of them are social media–like and designed to rapidly share content. Helo and TikTok are the most popular social media apps, along with short video and live-streaming apps like LiveMe, Vigo Video, BIGO LIVE, and Kwai. TikTok's expansion has been particularly noteworthy: having launched only in early 2018, the app had reached over a third of all Indian smartphone users by the end of 2019, with Indian users now accounting for a full third of TikTok's global user base.[55]

The Indian market for content, news, and social media is increasingly becoming a two-horse race, with China-based companies aggressively competing to dislodge the dominance of American digital platforms in India. This mirrors a broader trend of Chinese technology platforms and infrastructure proliferating around the world and unseating FAANG companies (Facebook, Apple, Amazon, Netflix, and Google) from their leadership positions. An obvious concern is whether Chinese platforms in international markets, especially those with skeletal or no data protection laws, will offer perfunctory privacy policies, but no concrete safeguards for handling user data. Especially worrisome is the possibility of Beijing "weaponizing" Chinese digital platforms in India for conducting disinformation campaigns during elections. The Communist Party's influence over state-owned enterprises is well documented, but relatively sparse attention has been paid to its growing sway over its private technology sector. Many major technology companies, including Tencent, Alibaba, and Baidu have a "party committee," and many co-operate with the CCP to build surveillance infrastructure within Beijing.[56] Not only does the proliferation of Chinese technology platforms then allow the Chinese state to shape global norms and practices around speech, data protection, and surveillance, it also gives the CCP the tools to potentially interfere in the domestic politics of nations heavily reliant on its platforms.

A. Focusing on Rural Markets

Three aspects of Chinese technology companies vis-à-vis their role in India's "digital public sphere" merit attention for their potential to be wielded as disruptors of India's political and electoral processes and institutions. First, these platforms focus overwhelmingly on demographics in Tier 2 and Tier 3 cities in India, whose political and social milieu receive relatively less scrutiny by India's Delhi-centric national media.[57] Chinese applications have picked up on a trend that American technology platforms either missed or refused to give importance to: both the absolute number of rural Indian internet users and the amount of time they spend on news, social media, and

[54] Shadma Shaikh, *The Chinese Takeover of Indian App Ecosystem*, Factor Daily (Jan. 2, 2019).

[55] Rebecca Bellan, *TikTok Is the Most Downloaded App Worldwide, and India Is Leading the Charge*, Forbes (Feb. 14, 2020).

[56] Chauncey Jung, *What Communists Do in China's Tech Companies*, Inkstone (Dec. 4, 2018).

[57] Mugdha Variyar, *How Chinese Apps Are Making Inroads in Indian Small Towns*, Economic Times (Aug. 10, 2018).

online entertainment exceeds their urban counterparts.[58] Chinese platforms have catered swiftly and remarkably to local and vernacular content in India. Helo, for instance, operates in at least fifteen Indian languages.[59] So do Chinese-owned news applications like UC News, which has a staggering 100 million downloads, and News Dog, with nearly 50 million downloads.[60] The result being Chinese applications serve as the primary source of news and content for an entire generation of rural youth coming online, with their practices and consumption trends largely invisible to India's national security community (which does not possess the tools or capacity to track disinformation even on larger platforms), and also to international watchdogs, who may not have the resources to track content in local Indian languages.

Compounding the problem is the limited information available on the extent to which these platforms have gathered data on Indian users and their behavior.[61] Although platforms like TikTok and Helo have been compelled to respond to data privacy concerns—variously promising to store data locally[62]—there is no institutional effort devoted to monitoring the full extent of China's data-gathering capabilities in India. India's draft data protection law, which envisages an independent Data Protection Authority to perform such regulatory oversight, is in the preliminary stages of parliamentary deliberation. Aggravating these risks are poor cyber hygiene practices in India, which were recently highlighted by the National Cyber Security Coordinator.[63]

B. The Popularization of Chinese Platforms

The second concern is the steady migration in India of online political content to Chinese platforms given their popularity. Despite multiple political outfits calling for a ban on Chinese platforms, many now have a strong presence on them.[64] As political content and rhetoric gain momentum on Chinese applications, their operations will have to grapple with disinformation that is par for the course for any campaign. This may well allow China to leverage Russia-style tactics that rely on accentuating social and political fault lines. This risk is exacerbated by the fact that, unlike Russia, Chinese actors own the platforms on which Indian political conversations are hosted and have

[58] Hello Holdings Limited, Helo, Mobile App, Version 3.2.4.02, *available at* https://play.google.com/store/apps/details?id=app.buzz.share&hl=en.

[59] UCWeb, UC News, Mobile App, Version 3.0.5.1080, *available at* https://play.google.com/store/apps/details?id=com.uc.iflow&hl=en.

[60] News Dog Team, News Dog, Mobile App, Version 2.8.1, *available at* https://play.google.com/store/apps/details?id=com.newsdog&hl=en.

[61] For an analysis of Huawei and Vivo's privacy policies as they pertain to India, *see generally* Arun Mohan Sukumar, *Working with "Last-Mile" Data Protection in India*, Policy Paper Asie Visions No. 96 (IFRI, 2017).

[62] Megha Mandavia, *China's ByteDance to Store Indian Data Locally after MPs Raise Concerns on Privacy, National Security*, Economic Times (July 22, 2019).

[63] Sandhya Sharma, *Concerned about Global Spurt in Cybercrimes, PMO's Cyber Chief Issues Cyber-Advisory for Online Users*, Economic Times (Apr. 10, 2020).

[64] Anumeha Chaturvedi, *Political Parties Plan to Up Tiktok Presence*, Economic Times (Dec. 3, 2019).

already acquiesced to hosting manipulated content. In fact, the key to the success of almost every major content app in China has been turning a blind eye toward "racy" content—whether it is doctored videos, edgy political caricature, or downright misinformation, and even pornography.[65] The most recent reports of false news on these platforms relate to the coronavirus, with a digital analytics firm identifying disinformation targeting India's Muslim community for ostensibly conspiring to spread the virus all over India.[66] Concerns around disinformation on Chinese applications even compelled the Madras High Court to ban TikTok, a judgment that was subsequently reversed.[67] Despite repeated calls by various political parties over the years, the growing popularity of Chinese platforms has compelled these parties to host political content on them.

Adding to this concern is the gradual absorption of Chinese platforms into the market for influencers and digital advertising—one that political outfits tap into for personnel and technical resources to run their campaigns. The director of a political campaign firm, for instance, was quoted as considering "TikTok very seriously for elections" and to "try to leverage it in a way that will not seem political."[68] Chinese applications are also heavily investing in creating a market for and network of influencers and celebrities,[69] many of whom are tapped by political parties during their campaigns. One TikTok influencer was even offered a party ticket by a national political party to run for state assembly elections in 2019.[70]

C. Content Moderation

A third concern relates to content moderation on these platforms. TikTok has already come under scrutiny in the United States for suppressing or censoring content outside Chinese borders. Last year, the app was accused of having instructed moderators to suppress material created by users "deemed too ugly, poor, or disabled for the platform."[71] Concerns were heightened in the United States by reports of other Chinese platforms, like WeChat, censoring political content in jurisdictions outside of China, especially in the Southeast Asian states where it is quite popular.[72] A recent forensic analysis by the Citizen Lab alleged WeChat also censors content of accounts that are not registered to China-based phone numbers.[73] In response, platforms like

[65] Shadma Shaikh, *The Chinese Takeover of Indian App Ecosystem*, Factor Daily (Jan. 2, 2019).

[66] Ankit Kumar, *Surge in TikTok Videos Aimed at Misleading Indian Muslims over Coronavirus Precautions*, India Today (Apr. 3, 2020).

[67] Richa Taneja, *Ban on TikTok Video App Lifted by Madras High Court*, NDTV (Apr. 24, 2019).

[68] Shanthi S., *Political Parties to Cash in on India's TikTok Mania for Election Ads*, INC42 (Dec. 3, 2019).

[69] Shadma Shaikh, *Chinese Apps Scramble for India's Kardashians*, Factor Daily (Mar. 27, 2018).

[70] Soumyarendra Barik, *TikTok Celebrity Gets BJP Ticket for Upcoming Haryana Elections*, Medianama (Oct. 7, 2019).

[71] Sam Biddle, Paulo Victor Ribeiro, & Tatiana Dias, *Invisible Censorship*, The Intercept (Mar. 16, 2020).

[72] Emily Feng, *China Intercepts WeChat Texts from U.S. and Abroad, Researchers Say*, NPR (Aug. 29, 2019).

[73] Jeffrey Knockel et al., *We Chat, They Watch—How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus* (The Citizen Lab, May 7, 2020), *at* https://citizenlab.ca/2020/05/we-chat-they-watch/.

TikTok have committed to outsource some of their content-moderation functions to jurisdictions outside of China—but the policy change seemingly applies only to the U.S. market.[74] As mentioned previously, China's ability to influence how content is ranked or censored in India has largely been ignored by state institutions and civil society. Stray media reports suggest that such actions have already taken place. When the deeply polarizing protests against the Citizenship Amendment Act first began in India in December 2019, for instance, moderators at BIGO Live were asked to "reduce visibility" of videos involving protest.[75] It is not clear yet how the India offices of Chinese platforms receive, create, or enforce these guidelines.

Although no authoritative finding or evidence of Chinese electoral influence operations in India has emerged, the preconditions to facilitate or enable such methods are certainly in place (just as they were ahead of Russia's influence operations in the 2016 American elections). China possesses a long history of information warfare and the digital tools and capacity to execute such operations, and has increasingly demonstrated a willingness to deploy these tools, although they have so far been limited to long-standing "core" interests relating to Hong Kong and Taiwan. As the next section highlights, however, there are demonstrable instances where it could turn on the "faucet" of disinformation campaigns in India, directing it against the country's political and electoral infrastructure.

V. Incentives for China to Interfere in India's Democratic Processes

The deep integration of China's social media platforms into India's digital public sphere as well as its evolving disinformation tactics animate concerns that China is now in a position to influence Indian political processes. This section will argue that China has also begun recently to exhibit its willingness to exercise these levers of influence, given the evolving nature of the bilateral relationship.

The China-India relationship has long been defined by a mix of conflict, competition, and cooperation. Even as they fought a limited boundary war in 1962, India and China have also partnered to jointly seek global governance reforms. Over the past decade, however, differences between both have been thrown into sharper relief, with the space for cooperation receding rapidly. These differences now extend across multiple domains and fronts. China has used its growing clout in multilateral institutions to work at cross-purposes with Indian interests, whether by pussyfooting UN Security Council Resolution 1267 committee sanctions on terrorist outfits based in Pakistan, or continuing to oppose India's entry into the Nuclear Suppliers Group (NSG).[76] In a similar vein, China has used economic largesse under the umbrella of the Belt and

[74] *TikTok to Stop Using China-Based Moderators to Monitor Overseas Content*, Wall Street Journal (Mar. 15, 2020).

[75] Prasid Banerjee, *Inside the Secretive World of India's Social Media Content Moderators*, Livemint (Mar. 18, 2020).

[76] *China Hints It Will Continue to Block India's Bid to Join Nuclear Suppliers Group*, Scroll (Jan. 31, 2019).

Road Initiative (BRI)[77] to try to displace India from its role as a hegemon in South Asia.[78]

Even so, India still occupies only a minor role in China's strategic calculus; it is seen largely as a regional competitor and dangerous only to the extent that it could support U.S. efforts to undermine China's rise.[79] This thinking is bound to change as India's economic rise and own evolving geopolitical calculations begin to affect China's national interests. Some trends to this effect are already visible. It is worth recalling that India was the first major country to have objected to the BRI, China's flagship twenty-first-century project to position itself as a global power, a move that catalyzed similar objections from the United States and European nations that were earlier ambivalent about the project.[80] Equally significant was India's ability to weather China's territorial aggression in Bhutan, an effort that culminated in the 2017 Doklam standoff.[81] Again, this episode marked a unique political moment in how India's foreign policy actions influenced China's global interests.[82] China has long used strong-arming tactics to expand territorial claims to the South China Sea, which have largely been successful. Doklam was perhaps the first instance where a major power intervened in the territory of a smaller state to thwart China's aggression.

It is clear a more muscular Indian foreign policy vis-à-vis China will compel Beijing to deploy new tools to mitigate India's influence and contain its rise. As its behavior in the United States, Europe, East Asia, and Australia demonstrates, China is no longer shy about wielding blunter instruments for political and electoral influence. It is necessary, then, to not only identify the tools China may use but also the political incentives that may encourage it to manipulate India's political processes.

A. Targeting Ethnic, Religious, and Social Fault Lines

We identify three major pathways. The first would be to exploit India's ethnic, religious, and social fault lines. In response to equivalencies drawn between the rise of India and China, Beijing has long argued that India's "messy" democracy would always make it an inferior power.[83] Under the Xi administration, China's rhetoric and ideological posturing against democracies have only sharpened. Indeed, China's

[77] For background on the Belt and Road Initiative, *see* Andrew Chatzky & James McBride, *China's Massive Belt and Road Initiative* (Council on Foreign Relations, Jan. 28, 2020), *available at* https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[78] Ashlyn Anderson & Alyssa Ayres, *Economics of Influence: China and India in South Asia* (Council on Foreign Relations, Aug. 3, 2015), *at* https://www.cfr.org/expert-brief/economics-influence-china-and-india-south-asia.

[79] Yun Sun, *China's Strategic Assessment of India*, War on the Rocks (Mar. 25, 2020); Andrew Scobell, *"Cult of Defense" and "Great Power Dreams": The Influence of Strategic Culture on China's Relationship with India*, in South Asia in 2020: Future Strategic Balances and Alliances 342 (Michael R. Chambers ed., 2002).

[80] Dhruva Jaishankar, *India Feeling the Heat on Belt and Road*, The Interpreter (Aug 21, 2017).

[81] For background on the 2017 Doklam standoff, *see Doklam Standoff: Explaining Two Months of Tensions between India and China*, Indian Express (Aug. 5, 2019).

[82] Oriana Skylar & Arzan Tarapore, *Countering Chinese Coercion: The Case of Doklam*, War on the Rocks (Aug. 29, 2017).

[83] *India's Messy Democracy Impediment in Race against China*, Deccan Herald (Jan. 19, 2015).

thinking on the matter has evolved over the past decade, beginning with the 2008 financial crisis and culminating with the political disruptions of Donald Trump and Brexit in 2016. Under Xi, China has expressed greater confidence about the failings of democratic systems and has offered "socialism with Chinese characteristics" as a viable political and economic alternative to emerging economies.[84]

India's economic and military rise as a major democratic power would dent the credibility of China's claims and would negatively affect its ideological and political standing in the near and far abroad.

Political entrepreneurship that harvests tensions among communities, especially along religious lines, has always been a feature of Indian democracy. However, much communal polarization and ethnic chauvinism has moved online with the advent of social media platforms. The cost of exploiting social cleavages has lowered, with digital spaces offering anonymity and deniability to political outfits. Multiple actors, local and foreign, have taken advantage of the digital medium to foment communal tensions in India.

Anecdotal evidence suggests China may well be in a position to similarly take advantage of India's social fault lines. In April 2020, for instance, reports emerged that Pakistan-based actors were posing as prominent political leaders and media personalities from the Middle East and amplifying content about the ruling BJP's mistreatment of Indian Muslims and insulting of Arab Muslim women in an effort to aggravate tensions between India's Hindu and Muslim communities.[85] At least one prominent fake account, pretending to be an Omani princess, was found to be followed by the People's Republic of China's MFA spokesperson Zhao Lijian.[86] Earlier in December 2019, reports indicated that over a thousand Twitter accounts based out of Pakistan were created to spread misinformation about India's polarized protests regarding the Citizenship (Amendment) Act, 2019.[87] One hashtag, #NaziIndiaRejected, was reportedly created by an organization called the Pakistan Tehreek-e-Insaaf Volunteer Task Force,[88] whose Twitter handle Zhao also follows.[89]

There is no evidence, at the time of writing, to indicate Chinese actors amplified, endorsed, or supported the creation of fake accounts or troll farms in Pakistan. However, Zhao's following of these accounts is not an insignificant matter. As the former deputy ambassador of the People's Republic of China to Pakistan, and now deputy director of the Chinese Ministry of Foreign Affairs Information Department, Zhao has been a vocal figure on—and savvy user of—social media. His tweets have previously been flagged by analysts, including former U.S. national security adviser Susan Rice, for attempting to exploit racial cleavages in Washington, D.C.[90] "Social media," Zhao has reportedly said, "is a weapon to counter [...] negative narratives."[91] As described earlier

[84] Jamil Anderlini, *China Is Taking Its Ideological Fight Abroad*, Financial Times (Jan. 9, 2020).

[85] Regina Mihindukulasuriya, *Many Arab Handles Slamming India Are Part of "Twitter War" from Pakistan*, The Print (Apr. 24, 2020).

[86] @Preetham_Offl, Twitter (Apr. 22, 2020, 11.27 AM), *at* https://twitter.com/preetham_offl/status/1252844364113432576?s=21.

[87] Sunny Sen, *Around 1,079 Pakistani Twitter Handles Being Used to Spread Hate Speech around Citizenship Amendment Act*, Firstpost (Jan. 8, 2020). For background on the Act and protests against the legislation, *see CAA—12 Key Points to Remember*, Press Information Bureau (Dec. 12, 2019); *Citizenship Amendment Bill: India's New "Anti-Muslim" Law Explained*, BBC (Dec. 11, 2019).

[88] *Id.*

[89] @PTI_VF, Twitter (Joined July 2016), at https://twitter.com/PTI_VF.

[90] Adam Taylor, *A Chinese Diplomat Had a Fight about Race in D.C. with Susan Rice on Twitter. Then He Deleted the Tweets*, Washington Post (July 16, 2019).

[91] Ben Smith, *Meet the Chinese Diplomat Who Got Promoted for Trolling the U.S. on Twitter*, Buzzfeed News (Dec. 2, 2019).

in this chapter, he has been one of the key promoters of the theory that the COVID-19 coronavirus not only originated in the United States but was also brought to Wuhan by the U.S. military.[92] Zhao has often cross-posted TikTok videos on Twitter, bringing to bear Chinese digital content on American platforms. His following of the malicious accounts in question can at best be described as an information-gathering exercise by a diplomat, but the fact that some of these accounts were recently created or altered for the explicit purpose of sowing discord among India's Hindus and Muslims suggests the matter necessitates further inquiry.[93]

Evidence from other parts of the world suggests autocratic states are increasingly leveraging their mutual disinformation networks and campaigns. India has already been a target of such operations. In October 2019, FireEye released a report documenting Iranian attempts at disinformation, which included nearly four thousand Hindi tweets that amplified typical Iranian foreign policy positions, including pro-Palestinian messaging and anti-Saudi Arabia or anti-U.S. content.[94] A forensic analysis of these operations by an independent cybersecurity consultant revealed at least four "Indian-sounding websites" were a part of the same Iranian networks, whose content was often shared on Indian social media with politically motivated hashtags, and were even retweeted and quoted by influential Indian political and media figures.[95] Evidence collected by researchers from the German Marshall Fund of the United States indicates Beijing is similarly "piggybacking off" this global network of propaganda networks by autocratic states—a development that could enable it to similarly exploit India's social fault lines without identification or attribution.[96]

B. Leveraging Pecuniary Interests

A second and potentially costly incentive for China would be to interfere in elections in Indian states where China has significant pecuniary interests. Beijing's strategy for political interference has evolved to take advantage of complex federal-state relations in democracies. In 2018, for instance, the Australian state of Victoria signed an MoU with China formally endorsing the latter's BRI. Canberra was caught off guard by the endorsement, was not consulted about the agreement, and had not even received a copy of its text (which was only made public after pressure from Prime Minister Scott Morrison).[97] The possibility of China attempting to influence subnational political

[92] Betsy Morris & Robert McMillan, *China Pushes Viral Messages to Shape Coronavirus Narrative*, Wall Street Journal (Apr. 10, 2020).

[93] *See* Mihindukulasuriya, *supra* note 85. The fake account of the Omani princess whom Zhao Lijian followed went earlier by the handle @Pak_Fauj and has since been deleted.

[94] Aria Thacker, *An Iranian Influence Campaign Has Been Targeting Indians on Twitter*, Quartz India (Nov. 2, 2018).

[95] Pukhraj Singh, *Planet-scale Influence Operation Strikes at the Heart of Polarised Indian Polity—Part I*, Writings of Pukhraj Singh (Nov. 26, 2018), *at* https://pukhraj.me/2018/11/26/planet-scale-influence-operation-strikes-at-the-heart-of-polarised-indian-polity/.

[96] *See* Jessica Brandt & Bret Schafer, *Five Things to Know About Beijing's Disinformation Approach* (German Marshall Fund Alliance for Securing Democracy, Mar. 30, 2020), *at* https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/.

[97] Paul Karl, *Scott Morrison Rebukes Victoria for Signing Up to China's Belt and Road Initiative*, The Guardian (Nov 6, 2018).

outcomes was apparent again in the U.S. state of Iowa, where the Chinese state–run *China Daily* ran a supplement in Iowa's largest newspaper outlining how the Trump administration's trade war would damage Iowa's large and profitable soybean trade with China.[98] These evolutions in China's political interference complement its economic statecraft, which have accelerated rapidly since the launch of the BRI.

Although India is not a signatory to the BRI, China's investments in India have nonetheless risen rapidly—with Beijing having invested a conservative $8 billion over the past three years alone.[99] Several Indian states now independently seek to attract investments from Beijing. As China's economic interests in Indian states deepen, so too will the stakes of managing India's political and business elite. Soon after China blocked India's bid for NSG membership in 2016, for instance, the Chief Minister of Madhya Pradesh—a key functionary of Modi's Bharatiya Janata Party—called for economic cooperation to continue despite political tensions.[100] He had reportedly just returned from a trip to China, where he aggressively lobbied for new investments in his state and even offered new industrial parks solely for Chinese investors.[101] Before India formally voiced its opposition to the BRI in May 2017, the then Chief Minister of Andhra Pradesh lobbied for the coastal city of Visakhapatnam to become a hub along the BRI.[102] During his 2016 visit to China, Pradesh also secured a deal with a Chinese firm to mine resources in a district where his party had failed to garner votes and had lost to the opposition in the 2014 general elections.[103] Reports indicate that the decision was based on the "spur of the moment" and that plans for such an investment had not been discussed earlier.[104] The episode is reminiscent of how Beijing bankrolled infrastructure projects in the constituency of then Sri Lankan Prime Minister Mahinda Rajapaksa in an effort to gain political currency.[105]

There are other means through which Beijing could attempt to curry favor among India's local leaders. Chinese companies, for instance, have also begun sponsoring foreign junkets for India's political and administrative elite, with Huawei reportedly having paid for telecom regulators to attend a conference on 5G in China.[106] Foreign junkets have been a useful tool for China in its efforts to buy political influence elsewhere, such as in Australia[107] and with municipal representatives in Canada.[108] Although such developments in the India-China relationship are still evolving, given that Chinese investments in India are still relatively low, evidence from around the

[98] *China Warns Iowa Soybean Farmers of "A President's Folly,"* S. China Morning Post (Sept. 24, 2018).

[99] Ananth Krishnan, *Following the Money: China Inc's Growing Stake in India-China Relations*, Brookings Institution India Center 5 (Impact Series 032020-01, 2020).

[100] Sarah Watson, *India's Centre-State Divide on China* (Observer Research Foundation, July 11, 2016), *at* https://www.orfonline.org/expert-speak/indias-centre-state-divide-on-china/.

[101] *Id*.

[102] Sandeep Kumar, *Naidu Wants China to Take the Silk Route via Visakhapatnam*, The Hindu (Nov. 23, 2015).

[103] *Naidu Gets China into AP's Kadapa District in Astute Political Move*, Asianetnews (June 27, 2016).

[104] *Id*.

[105] *China's Xi Offers Fresh $295 Million Grant to Sri Lanka*, Reuters (July 22, 2018).

[106] *Don't Let Telecom Officials Go on Huawei-Sponsored Trip to China, RSS Affiliate Urges PM Modi*, Business Today (July 31, 2019).

[107] *China Telco Biggest Sponsor of MP Junkets*, SBS News (June 26, 2019).

[108] Sam Cooper, *Canadian Mayors May Have Unwittingly Been Targets of Chinese Influence Campaign*, Global News (Mar. 9, 2020).

world suggests that Beijing's attempts to buy political influence often increase in scale and intensity. Once entrenched, they provide a lever for China to influence political and electoral outcomes in India's states, either to defend narrow pecuniary interests or to navigate anti-China sentiment at the federal level through the state administrations.

The numerous languages in which Chinese social media platforms operate in India provide a crucial vector for influence operations in local elections. Reports suggest that China has actively sought in the past to infiltrate the communications of India's strategic and diplomatic establishments. In 2015, Chinese actors targeted government, scientific, educational, and diplomatic institutions in India to steal information through phishing operations.[109] Earlier in 2009, India's then National Security Adviser M.K. Narayanan revealed his office was targeted in a cyber intrusion by Chinese actors.[110] It is worth recalling that attempts to influence the French election saw hackers release dozens of real and fake emails to smear Emmanuel Macron—not to mention the storied history of the use of *kompromat* by Russia in blackmailing foreign figures.[111] Although Beijing has not employed such tactics previously in India, its influence operations are continuously evolving: should Chinese actors possess sensitive information about India's political elite, it has, through the embedding of Chinese digital platforms in vernacular content, an effective conduit to perpetrate disinformation campaigns against their targets.

C. A Full-Court Press?

Finally, China could also attempt a full-court press, Russia-style operation to undermine Indian general elections in the future. This would certainly be an extraordinary development in global politics—but as China's actions in Taiwan show, Beijing is increasingly inclined to overlook public opinion to secure its regional and global interests, some of which have been detailed in this chapter. Should a political leader with a vocal and effective "anti-China" electoral platform emerge, Beijing may well attempt to undermine his or her bid for office. Signs of discomfort are already visible in Beijing with the Modi administration. In February 2014, Narendra Modi called on Beijing to "shed its expansionist mindset" while campaigning in the state Arunachal Pradesh, a territory over which Beijing has long claimed suzerainty.[112] Later in 2016, China took issue with the Indian government permitting the Dalai Lama to visit Tawang, a city in Arunachal Pradesh. At the time, China's MFA objected to this move by claiming that India is providing "a stage for anti-China separatist forces," further warning that it would "only damage peace and stability of the border areas and bilateral relations."[113] Similarly, in the 2019 general elections, a key state leader from the BJP claimed that

[109] Neha Alawadhi, *Chinese Hackers Targeting Indian Institutions for Data on Border Disputes, Diplomatic Matters: Report*, Economic Times (Aug. 22, 2015).

[110] *Chinese Made a Bid to Hack Our Computers, Says Narayanan*, Times of India (Jan. 19, 2010).

[111] Julia Ioffe, *How State-Sponsored Blackmail Works in Russia*, The Atlantic (Jan. 11, 2017).

[112] *China Should Shed Expansionist Mindset: Modi*, The Hindu (Feb. 22, 2014).

[113] People's Republic of China, Ministry of Foreign Affairs, *Foreign Ministry Spokesperson Lu Kang's Regular Press Conference* (Oct. 29, 2016), *at* https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1411259.shtml.

China had "retreated for the first time"[114] under the leadership of Narendra Modi, a less-than-subtle reference to the Doklam standoff to which China's state-run *Global Times* took objection.[115]

There are other sources of tension in the bilateral relationship under Modi's watch, most notably on account of India's participation in the resuscitated "Quadrilateral Initiative" and for its advocacy of a new geographical construct in Asia, the "Indo-Pacific." China sees both Indian initiatives as an effort to contain its rise, and has repeatedly warned through its state media of the consequences of India's warming ties with the United States.[116] The political constituencies that the Narendra Modi government leans on to win elections are also unfavorably disposed toward China. The Rashtriya Swayamsevak Sangh, the ideological progenitor of the BJP, has remained vehemently anti-China over the course of the BJP administration. It opposed India's entry into the Regional Comprehensive Economic Partnership because it was "China-led."[117] It has also been vocal about preventing China's telecom companies from establishing a foothold into the Indian 5G market.[118] Most recently, the Modi administration introduced new economic restrictions against Beijing, mandating government scrutiny and approvals for *all* Chinese investments.[119] In this context, it is conceivable that China's influence operations in Taiwan, which were designed to undermine the electoral bid of a candidate who was inimical to Chinese interests, may well foreshadow similar campaigns in India.

VI. Conclusion: The Widening Canvas of China's Influence Operations

As its global ambitions expand, China will likely shift from issue-based influence operations and disinformation campaigns (the BRI, the COVID-19 pandemic, protests in Hong Kong SAR and Taiwan) to more systemic ones targeting electoral and political infrastructure, especially in democracies. The calculus is apparent enough: Why expend resources on propaganda to sell American states on freer trade, when they could be mobilized to unseat the federal administration that is pursuing the "trade war" with Beijing? Emerging markets, too, have witnessed a progressive consolidation of political power by federal governments—the trend has been visible in several countries, including Brazil, India, Malaysia, Indonesia, Turkey, the Philippines, and Sri Lanka. This development presents China with the opportunity to target key political figures and outfits through digital platforms, with a view to steer entire electoral outcomes. No longer can states, advanced or developing, count on Western social media platforms alone to detect and weed out online influence operations guided by

[114] Yogi Adityanath, *China Retreated for First Time under PM's Leadership*, NDTV (Apr. 6, 2019).
[115] Zhao Gancheng, *Modi Playing China Card to Win Election*, Global Times (Apr. 29, 2020).
[116] *America's Indo-Pacific Strategy Will Cost You: China to India*, Economic Times (July 2, 2018).
[117] Neelam Pandey, *RSS Affiliate Claims Modi Govt Not Keen on RCEP Trade Deal But Civil Servants Pushing It*, The Print (Oct. 15, 2019).
[118] *RSS-Affiliated Body Writes to PM Modi against Huawei's 5G Trial in India*, NDTV (Dec. 31, 2019).
[119] *One Eye on China, Modi Govt Tweaks FDI Policy to Curb "Opportunistic Takeover" of Indian Companies*, The Wire (Apr. 18, 2020).

Beijing. China's own powerful technology companies have made significant inroads into foreign markets, gradually moving up the value chain: starting out as purveyors of physical infrastructure, they are now curators of digital content. In March 2020 alone, at the height of the COVID-19 pandemic, TikTok saw 12 million Americans join the platform—a number equal to its entire subscription base in the United States till just a few months ago.[120] The average American user spent five hours on Instagram and eight hours on TikTok in the same month.[121] An extraordinary displacement of U.S. digital platforms by Chinese companies is underway on its home turf, creating ever more vectors of (and constituencies for) influence operations led by China. Just as China has relied on disinformation networks of other autocratic states, Chinese platforms popular in Western democracies could be used as slingshots for election interference by China.

For developing economies like India, the picture is even more grim. India is reliant on the continued economic growth of China for its supply chains and investments, at least for the near future. Its digital economy has been effectively propped up by Chinese technology companies selling cheap handheld devices. Economic imperatives around 5G and foreign direct investment cannot be easily dismissed, no matter how vexatious the security dilemmas of Chinese involvement in highly sensitive sectors and industries. Even as a delicate bilateral dance ensues, India will encounter aggressive and bold influence operations from across its eastern border.

This chapter offers an analytical framework to study Chinese campaigns targeting India's election infrastructure and political processes through digital channels. A few policy prescriptions to help monitor and tackle such campaigns follow:

1. *Map the dimensions and magnitude of influence operations*. Federal and state election commissions in India have limited capacity to monitor foreign interference in democratic processes. The Election Commission of India appointed a chief information security officer (CISO) in December 2017 to assess cyber threats against polling infrastructure and offer guidelines on "social media security," broadly defined.[122] The incumbent CISO is a former official of India's National Intelligence Grid.[123] Meanwhile, state election commissioners have also appointed Cybersecurity Nodal Officers (CSNOs), who report directly to the CISO. While the CISO has done a commendable job in identifying the nature of cyber threats to India's election infrastructure and communicating them to state-level officers through "advisories,"[124] the flow of information can tend to be top-down. The CISO should curate an interagency platform comprising CSNOs, intelligence officials, and law enforcement agencies across the country, that periodically evaluates the scale and intensity of influence operations, including by

[120] Daniyal Malik, *Data Shows that U.S. Consumers Are Loving the TikTok during the COVID-19 Pandemic*, Digital Information World (May 4, 2020).
[121] *Id*.
[122] Election Commission of India, *Appointment of Chief Information Security Officer (CISO) at Election Commission of India* (Dec. 27, 2017), *at* https://eci.gov.in/files/file/1841-appointment-of-chief-information-security-officer-ciso-at-election-commission-of-india/.
[123] *Dr. Kushal Pathak*, LinkedIn (May 29, 2020), *at* https://in.linkedin.com/in/kushalpathak.
[124] *See* Election Commission of India, *supra* note 9.

Chinese actors. Maintaining an information-sharing network between federal and state agencies is an important first step in tackling foreign election interference. Particularly essential is building capacity to monitor foreign influence operations in vernacular languages through platforms like TikTok, which an interagency platform would be well poised to do.

2. *Support and champion initiatives like the Paris Call for Trust and Security in Cyberspace*. The Paris Call of November 2018 seeks to enhance the capacity of state and nonstate actors "to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities."[125] India is not formally a "supporter" of this nonbinding instrument. New Delhi's championing of such multistakeholder initiatives is essential both on account of its democratic credentials and rising prominence as one of the world's largest digital economies. Instruments like the Paris Call create soft "norms" or "rules of the road" against foreign election interference that are gradually embedded into the practice of states and private technology companies.
3. *Elevate the role of Chinese platforms to the high table of bilateral dialogue*. Despite political tensions apparent in their relationship, India and China have sustained high-level contact over the years. Prime Minister Narendra Modi and President Xi Jinping have met for two "informal summits" in Wuhan (2018) and Mamallapuram (2019)—meetings that have no slated deliverables or joint statements, giving both leaders the flexibility to discuss virtually any matter relevant to bilateral ties.[126] Cybersecurity concerns posed by Chinese technology platforms, despite their ubiquitous presence in India's digital economy, do not appear to have been addressed in these discussions.[127] Huawei's potential role in providing 5G telecommunication infrastructure in India, and its attendant security implications, has acquired considerable political visibility and could likely feature as a talking point in the next informal summit. The issue of foreign election interference routed through, or facilitated by, Chinese technology platforms should also be flagged by New Delhi at this forum. The popularity of Chinese apps and devices in India is certainly a strategic asset for Beijing were it to mount an election interference campaign. However, the reputational costs for Chinese technology companies—given their stake in the Indian digital economy—associated with being conduits for influence operations are equally significant. New Delhi should raise those costs by heightening the visibility of election interference as an issue in bilateral discussions.

This chapter has argued Chinese digital influence operations in India could exploit (1) the country's existing socioeconomic fault lines; (2) federal-state tensions; and (3) the messy and chaotic nature of its general election, traditionally held over several "phases" and weeks in the summer. As India becomes more vocal in its opposition to

[125] *The Paris Call for Trust and Security in Cyberspace* (Nov. 12, 2018), *at* https://pariscall.international/en/call.

[126] Devirupa Mitra, *Explainer: Ahead of Modi-Xi Informal Summit, Key Questions Answered*, The Wire (Oct. 10, 2019).

[127] Ministry of External Affairs, Government of India, *2nd India-China Informal Summit*, *at* https://www.mea.gov.in/press-releases.htm?dtl/31938/2nd_IndiaChina_Informal_Summit.

China's global projects, such operations are likely to intensify in frequency and scale. The theaters of influence operations too may shift, blurring the line between domestic and foreign campaigns. Twitter handles of Chinese embassies and consulates in Paris and Kolkata are today vehicles for disinformation campaigns pitting China favorably against the United States.[128] As the Indian footprint in global affairs enlarges, New Delhi should be prepared to meet challenges from China to the integrity of its democratic processes not only at home but also abroad.

[128] @AmbassadeChina, Twitter (Apr. 30, 2020, 8.24 PM), at https://twitter.com/ambassadechine/status/1255873178632687622?s=21; Mark Scott, *Chinese Diplomacy Ramps Up Social Media Offensive in COVID-19 Info War*, Politico (Apr. 29, 2020).