Challenging China's Bid for App Dominance

Kristine Lee and Karina Barbesino

BLUNTING CHINA'S AUTHORITARIAN TOOLKIT

Center for a New American Security

EXECUTIVE SUMMARY

Social media platforms are emerging as central to China's efforts to shape the global information architecture. Beijing is exploiting the relative openness of the United States' and other democracies' social media platforms to manipulate the narrative around its policies, while the virality of some of China's own social media applications (colloquially known as "apps") has positioned Beijing to quietly export its model of surveillance and censorship. Social media platforms will continue to be an important vector by which information is disseminated and consumed, and control over these platforms will yield significant influence over perceptions of the United States and China.[1] As Beijing executes a more aggressive global social media strategy, the U.S. government should coordinate closely with both like-minded countries and social media companies to backstop the integrity, transparency, and competitiveness of their own platforms.

CHINA'S SOCIAL MEDIA PLATFORMS: A NEW INSTRUMENT OF NATIONAL POWER

Just a decade ago, American companies dominated the global social media ecosystem. Facebook had already captured a billion users across more than 200 countries by 2012 while many of China's popular "super apps"—which bundle several different services under a single interface—were either nonexistent or marginal players.[2] But today, the gap between the userbases of American and Chinese platforms appears to be closing. Facebook-owned WhatsApp, for example, currently has about 1.5 billion users globally,[3] while WeChat—a messaging app that the Chinese tech giant Tencent created in 2011—has already captured 1.08 billion users globally, though principally within China's borders.[4]

Tencent led a concerted push in the past several years to not only centralize a full suite of features under a unified platform (namely, WeChat) but to also expand its international userbase including through by the launch of English and other non-Chinese language versions of the platform in 2012.[5] After reaching nearly 95 percent saturation in Tier 1 Chinese cities,[6] WeChat is gaining a foothold across South and Southeast Asia as well as Latin America. Tencent has leveraged China's diaspora and outbound tourist population, which relies on WeChat Pay for digital

1. For a comprehensive look at China's information influence operations, see Rush Doshi, "China Steps Up its Information War in Taiwan," *Foreign Affairs*, January 9, 2020, https://www.foreignaffairs.com/articles/china/2020-01-09/china-steps-its-information-war-taiwan.

2. Felix Richter, "How Facebook grew from 0 to 2.3 billion users in 15 years," World Economic Forum, February 5, 2019, https://www.weforum.org/agenda/2019/02/how-facebook-grew-from-0-to-2-3-billion-users-in-15-years.

3. Sahir Farid, "WhatsApp Usage, Revenue, Market Share and other Statistics (2019)," Digital Information World, February 11, 2019, https://www.digitalinformationworld.com/2019/02/whatsapp-facts-stats.html.

4. Mansoor Iqbal, "WeChat Revenue and Usage Statistics (2019)," Business of Apps, February 27, 2019, https://www.businessofapps.com/data/wechat-statistics/.

5. Mohit Mittal, "WeChat—The One App That Rules Them All," Digital Initiative, August 25, 2017, https://digital.hbs.edu/innovation-disruption/wechat%E2%80%8A-%E2%80%8Athe-one-app-rules/.

6. China's dynamic class-tier classification system categorizes its cities into four tiers. Tier 1 cities are typically the largest, wealthiest, and most populous cities, such as Beijing, Guangzhou, Shanghai, and Shenzhen.

BLUNTING CHINA'S AUTHORITARIAN TOOLKIT

payments, to penetrate emerging markets. This strategy has proven effective in Malaysia, for example, where WeChat Pay MY is already one of the country's top licensed e-wallet operators only a year after market entry.[7]
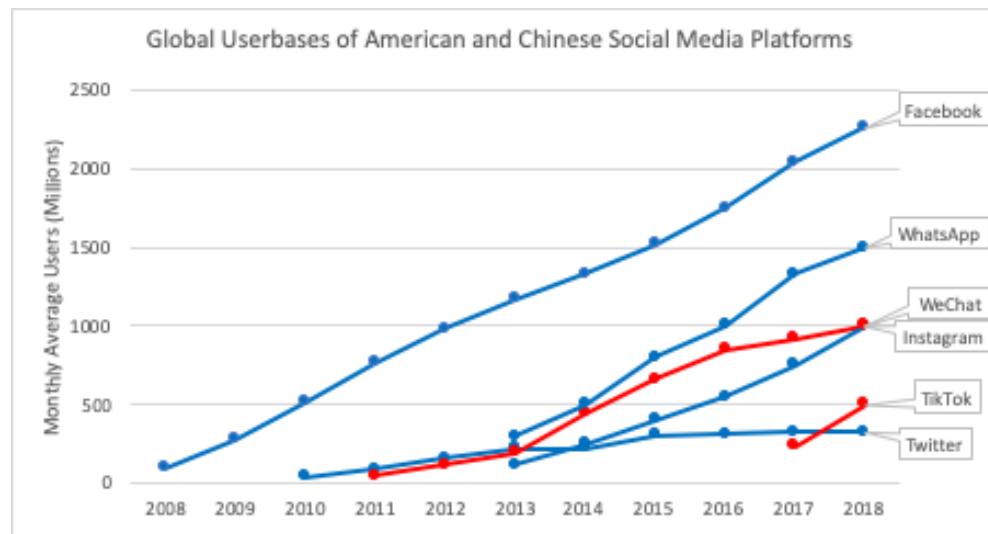
While American platforms still dominate, the growing prominence of Chinese-owned social media apps such as TikTok and WeChat, particularly in emerging markets, suggests that the gap may be closing in the years ahead. Source: Esteban Ortiz-Ospina, "The Rise of Social Media," Our World in Data, Sep 18, 2019, https://ourworldindata.org/rise-of-social-media.

The rise of China's social media platforms has notable geopolitical implications. The Chinese Communist Party (CCP) has already dedicated considerable resources—through censorship, propaganda, public diplomacy, and strategic messaging both on its own and American platforms—to promote narratives about its inevitable ascent and the United States' relative decline, safeguard its self-proclaimed "core interests" such as Taiwan, and forestall criticism of its policies toward Hong Kong, Tibet, and Xinjiang.[8]

Beijing's efforts to shape the information environment beyond its borders have grown more pronounced over the past decade. Not long after becoming the General Secretary of the CCP, Xi Jinping declared in a speech at the August 2013 National Meeting on Propaganda and Ideology that for China to spread new ideas to developing countries it needed to "strengthen media coverage… use innovative outreach methods…tell a good Chinese story, and promote China's view internationally."[9] In 2015, the reorganization of the People's Liberation Army[10] and the consolidation of its cyber capabilities into a single service produced significant momentum for Beijing's concept of "information warfare," including the development and deployment of new platforms.[11] In 2019, as Beijing's control over Hong Kong seemed to grow tenuous, China's internet regulator (the Cyberspace Administration of China), its state-owned news agency (China News Services), and its Ministry of Foreign Affairs (MOFA) began awarding contracts totaling more than $1 million aimed at expanding Beijing's global social media presence.[12]

7. ESC Editorial Team, "A deep insight into WeChat Pay's global expansion strategy," Ecommerce Strategy China, May 2019, https://www.ecommercestrategychina.com/column/a-deep-insight-into-wechat-pays-global-expansion-strategy; and Preetam Kaushik, "The new frontier: Malaysia is WeChat's stepping stone to Southeast Asian markets," *ASEAN Today*, April 6, 2019, https://www.aseantoday.com/2019/04/the-new-frontier-malaysia-is-wechats-stepping-stone-to-southeast-asian-markets/.

8. Ben Blanchard and Andrew Heavens, "U.S. 'Smears' of China Affecting Global Stability, Top Beijing Diplomat Says," *The New York Times*, December 23, 2019, https://www.nytimes.com/reuters/2019/12/23/business/23reuters-china-usa.html.

9. Anne-Marie Brady, "Authoritarianism Goes Global (II): China's Foreign Propaganda Machine," *Journal of Democracy*, 26 no. 4 (October 2015), 51–59.

10. Ministry of National Defense, *China's Military Strategy*, May 26, 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.

11. The State Council, *China's National Defense in the New Era*, July 24, 2019, http://english.www.gov.cn/archive/whitepaper.

12. "China's propaganda machine is spending over $1 million to buy influence on foreign social media," Quartz, August 21, 2019, https://qz.com/1691785/chinas-paying-to-build-its-influence-on-foreign-social-media/.

Center for a New American Security
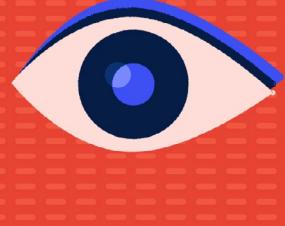
BLUNTING CHINA'S AUTHORITARIAN TOOLKIT

A few key trendlines have emerged from Beijing's recent efforts:

— **As Chinese-designed and marketed apps proliferate beyond China's borders, the CCP can mobilize its information operations more nimbly and covertly.** The CCP is positioned to quietly export its model of content curation and censorship to global, including American, audiences. Preliminary analysis, for example, suggests that content on TikTok—one of the world's fastest-growing social media platforms and the most downloaded app worldwide in the first quarter of 2019[13]—may be subject to China's censorship apparatus by way of its Beijing-based parent company, ByteDance.[14] And the censorship concerns around WeChat are already well-documented.[15] During the protracted pro-democracy struggle in Hong Kong in 2019, the CCP's censorship machinery hummed along at full throttle as Tencent suspended the accounts of WeChat users, even in the United States, who criticized Beijing.[16]

— **Beijing has sought to shape the narrative around its policies and interests through the propagation of false information and the flooding of content by state-controlled bots and commentators.[17]** Following Twitter's removal of 936 accounts and suspension of 200,000 others originating from China that sought to discredit the protests in Hong Kong, Beijing has sought to flip the script, rebutting criticism of its practices with the accusation that U.S. platforms are censoring legitimate views held by Chinese people.[18] Beyond China's borders, Chinese state actors have, for example, used WeChat to mobilize the Chinese diaspora to take to polling stations during Canada's 2019 federal election, which potentially foreshadows how the CCP might leverage WeChat for more directive influence for or against certain candidates in future democratic elections.[19] There has also been a proliferation of Chinese apps—such as Zao, Yanji, and now a pending feature within TikTok[20] dubbed "Face Swap"—that allow users to create low-quality deepfakes in mass quantities.[21] These apps would pose significant risks to democratic societies if they gain traction, as the virality of videos will ensure that they move more quickly than governments' ability to confirm or deny their verity.

— **Concerns around espionage and data harvesting stemming from Chinese apps have grown more acute, particularly among political activists critical of Beijing's policies and in countries suspicious of China's ambitions.** In 2019, for example, various CCP organs harvested the personal information of dissidents in Hong Kong from their social media profiles and publicly released their personal data through social media platforms and websites including "HK

13. "Top Apps Worldwide for Q1 2019 by Downloads," Sensor Tower Blog, May 15, 2019, https://sensortower.com/blog/top-apps-worldwide-q1-2019-downloads.

14. Geoffrey Gertz, "Is TikTok a threat to national security?" *The Washington Post*, November 11, 2019, https://www.washingtonpost.com/politics/2019/11/11/is-tiktok-threat-national-security/.

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

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

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

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

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

20. Peter Suciu, "TikTok's Deepfakes Just the Latest Security Issue for the Video Sharing App," *Forbes*, January 7, 2020, https://www.forbes.com/sites/petersuciu/2020/01/07/tiktoks-deepfakes-just-the-latest-security-issue-for-the-video-sharing-app/#570476e870a2.

21. Colum Murphy and Zheping Huang, "China's Red-Hot Face-Swapping App Provokes Privacy Concerns," Bloomberg, September 1, 2019, https://www.bloomberg.com/news/articles/2019-09-02/china-s-red-hot-face-swapping-app-provokes-privacy-concern.

Center for a
New American
Security
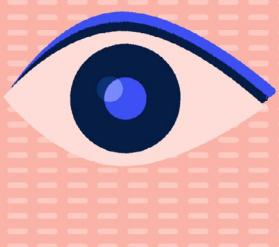
Leaks," a website that is notably hosted on a Russian domain.[22] Meanwhile, data collection through Chinese apps has also raised the specter of hard security risks for some countries. In 2017, the Indian Intelligence Bureau directed troops stationed at the Indian and Chinese border to uninstall 42 Chinese apps, including WeChat, Truecaller, and Weibo, among others, due to cyber espionage risks that could gravely threaten India's security in a military contingency along what remains a disputed border.[23] And concerningly for American users, preliminary assessments have revealed major flaws in TikTok's data security practices.[24]

— **Beijing is exploiting the lack of reciprocity between the information ecosystems of China and democracies to advance its agenda.** While American social media platforms are increasingly difficult to access within China's borders, especially since the CCP's crackdown on virtual private networks in the lead-up to its 2017 Party Congress,[25] Beijing is permeating the United States' userbase with its own viral apps while using Twitter and Facebook to conduct strategic messaging beyond its borders.[26] Even Chinese diplomats have taken to Twitter, with the Chinese Ministry of Foreign Affairs opening an official Twitter account in December 2019. Shortly after her promotion to the position of Director of the MOFA Information Department, for example, Hua Chunying outlined a more aggressive global social media strategy in a Study Times article which suggested that Twitter may become an important tool in Beijing's information warfare arsenal.[27] Finally, Beijing is using its economic heft to pressure American companies to acquiesce to its demands. Apple Inc., for example, controversially removed from its store the app HKmap.live, which helped Hong Kong protesters track police movements after a Chinese state newspaper criticized the U.S. technology giant for allowing the software to live on its platform.[28]

A RENEWED U.S. APPROACH TOWARD PLATFORM INTEGRITY AND DOMINANCE

The United States is entering a consequential year in its democracy, with a presidential election in November that will yield enduring implications for the country's policies toward China.[29] Against this backdrop, sustaining the integrity of American platforms and the free flow of information unfettered by state-endorsed censorship, false content promotion, and data harvesting is critical. The following recommendations are intended to guide U.S. policy—in both the near- and long-term future—as Beijing steps up its campaign to reconstitute the global information environment:

1. **Dial up pressure on U.S. social media companies to move toward faster and more transparent models of revealing and explaining state-directed influence activities on their platforms.** Members of the public and civil society would benefit from a more granular understanding of how Beijing is leveraging

22. Jane Li, "Russia is Beijing's best ally in the disinformation war against Hong Kong," Quartz, December 11, 2019, https://qz.com/1765092/russia-is-beijings-ally-in-media-war-against-hong-kong/; and DFRLab, "Telegram channels used to doxx and report Hong Kong protesters to Chinese authorities," Medium, September 25, 2019, https://medium.com/dfrlab/telegram-channels-used-to-doxx-and-report-hong-kong-protesters-to-chinese-authorities-91bed151f345.

23. Taruka Srivastav, "India's Intelligence Bureau urges troops to delete Chinese apps such as UC Browser and WeChat due to security risk," The Drum, November 30, 2017, https://www.thedrum.com/news/2017/11/30/indias-intelligence-bureau-urges-troops-delete-chinese-apps-such-uc-browser-and.

24. Ronen Bergman, Sheera Frenkel, and Raymond Zhong, "Major TikTok Security Flaws Found," *The New York Times*, January 8, 2020, https://www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html?auth=login-email&login=email.

25. Harry Krejsa, "Under Pressure: The Growing Reach of Chinese Influence Campaigns in Democratic Societies" (Center for a New American Security, April 2018), https://www.cnas.org/publications/reports/under-pressure.

26. Raymond Zhong, Steven Lee Myers, and Jin Wu, "How China Unleashed Twitter Trolls to Discredit Hong Kong's Protesters," *The New York Times*, September 18, 2019, https://www.nytimes.com/interactiv e/2019/09/18/world/asia/hk-twitter.html.

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

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

29. A number of critical U.S. allies and partners will also be facing elections this year, including South Korea, New Zealand, Hong Kong, Israel, and Taiwan with its presidential election earlier this month.

BLUNTING CHINA'S AUTHORITARIAN TOOLKIT

social media platforms to shape democracies' information environments. Facebook's collaboration with the Social Science One and Social Science Research Council to provide researchers with access to Facebook data sets was a positive first step at the time of its announcement in 2019,[30] but technical barriers to anonymizing data sets ultimately stymied these efforts.[31] Congress should increase pressure on social media companies—including through a regular series of public hearings and private briefings—to develop a streamlined process for providing researchers, analysts, and other members of civil society with access to data sets in ways that preserve users' privacy.

2. **Establish a data-sharing mechanism to pool information among U.S. allies on Chinese influence activities on social media platforms in a secure manner that protects people's privacy.[32]** This could begin with the creation of a rapid response cell, housed within the Federal Bureau of Investigation, that integrates a network of civil society and private sector representatives to partner with fact-checking centers across Five Eyes countries.[33] Currently, countries at the frontlines of combatting Chinese influence activities such as Taiwan, have relatively diffuse disinformation reporting structures scattered across government agencies. A more centralized, interagency model with a single coordinating head would be conducive to rapid response and ensuring all strategies and responses are appropriately funded.

3. **Execute a public diplomacy campaign to communicate to American and international consumers how the CCP can leverage Chinese-owned social media apps—and American platforms—to harvest data, facilitate censorship, and enable the spread of false information.** The Global Engagement Center could also partner with think tanks and other civil society entities to launch a streamlined campaign to raise public awareness about the ownership structures of viral Chinese-owned social media apps, such as TikTok. Senior U.S. government officials should leverage American social media platforms—including YouTube, Facebook Live, Twitter video clips, and LinkedIn Live—to explain to publics why Chinese influence and censorship activities on U.S. and Chinese platforms threaten democracies. This should be part of a broader U.S. effort to, with a coalition of like-minded countries in international organizations and other multilateral fora, increase pressure on Chinese social media companies operating internationally to adhere to the norms of the democratic societies in which they operate.[34]

4. **Prioritize educational investment in K-12 civics curricula that promotes digital literacy and critical thinking about information consumption among younger generations of Americans.** As social media usage pervades society and daily life, the American public's ability to correctly identify and react to false information will continue to be a challenge. The U.S. government should learn from other democracies' approaches to digital literacy, to invest in education strategies that will pay dividends for generations to come. Finland's multi-pronged approach, which couples educating young citizens about the importance of voting rights with a digital literacy "toolkit" and a critical thinking curriculum designed for news consumption, offers one such model.[35]

30. Facebook, Inc., "First Grants Announced for Independent Research on Social Media's Impact on Democracy Using Facebook Data," accessed December 26, 2019, https://about.fb.com/news/2019/04/election-research-grants/.

31. Jeffrey Mervis, "Privacy Concerns could Derail Unprecedented Plan to use Facebook Data to Study Elections," *Science*, September 24, 2019, https://www.sciencemag.org/news/2019/09/privacy-concerns-could-derail-unprecedented-plan-use-facebook-data-study-elections.

32. This recommendation was inspired by a recommendation advanced by CNAS Fellow Kara Frederick in her June 2019 report, see Kara Frederick, "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight," (Center for a New American Security, June 2019), https://www.cnas.org/publications/reports/the-new-war-of-ideas.

33. Kara Frederick, "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight."

34. Yaqiu Wang, "How China's censorship machine crosses borders—and into Western Politics," *The Washington Post*, February 20, 2019, https://www.washingtonpost.com/opinions/2019/02/20/how-chinas-censorship-machine-crosses-borders-into-western-politics/.

35. Eliza Mackintosh, "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy," CNN, May 2015, https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

Center for a New American Security
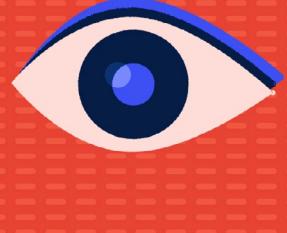
BLUNTING CHINA'S AUTHORITARIAN TOOLKIT

5. **Publicize existing software solutions for consumers, both within the United States and abroad, to guard against the spread of false information on American social media platforms.** There are already several software solutions that are either under development or functional at a limited scale that can notify social media users of instances of disinformation. The Duke Videofactchecking Tool, for example, is a browser extension under development that is geared toward providing live fact checking of information on television.[36] The U.S. government should amplify existing automated solutions that consumers, both at home and abroad, can leverage to identify instances of the CCP's and other state actors' use of social media to spread false information. As these tools become more effective, the U.S. government could require that major browsers include them as extensions that are, by default, enabled.

6. **Jumpstart innovation around designing scalable solutions for combatting the spread of false information on social media platforms.** In parallel with promoting existing solutions, the Defense Advanced Research Projects Agency should organize a "Disinformation Hackathon" for innovators in U.S. and ally countries to foster innovation around solutions for combatting state-sponsored information operations on their social media platforms. Cross-sectoral teams of participants could create new solutions to public challenges by leveraging open government datasets, as well as open-source information drawn from other sectors. To develop these tools and foster further innovation, the U.S. government should expand the sources of technology funding to include foreign governments, foundations, and the private sector.[37]

7. **Launch a "truth" campaign that widens the aperture of Chinese-language news sources and supports independent journalism and reporting on the CCP's digital influence activities.** The United States should expand and diversify its toolkit for communicating directly with Chinese-language populations, including by developing Chinese language websites and social media accounts to shed light on instances of state-organized disinformation activities, corruption, and human rights abuses. The U.S. Agency for Global Media (formerly the Broadcasting Board of Governors) should repurpose Radio Free Asia to report on new media and social media platforms and expand its scope to include language services for Central and South Asia to offer alternative sources of information in countries that receive significant Chinese infrastructure investment. The U.S. government should develop a more robust Fulbright Scholars exchange program for journalists from countries at the frontlines of Chinese influence campaigns to train at American universities and media centers, as well as for American journalists to travel to and provide independent reporting about CCP activities within those countries.

8. **Strengthen the branding and overall competitiveness of American and other democratic countries' social media platforms in third markets.** American and other democracies' technology and social media companies will cede ground to Chinese companies when they do not compete effectively in critical markets, such as in South and Southeast Asia, where social media penetration rates are experiencing steep growth.[38] U.S. social media companies should strengthen their branding in these countries through more aggressive outreach, connectivity, and partnership programs with local entrepreneurs and small and medium enterprises. They could also partner with American universities—such as the Massachusetts Institute of Technology, which already

36. RAND, "Tools That Fight Disinformation Online," accessed December 26, 2019, https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

37. Richard Fontaine and Will Rogers, "Internet Freedom: A Foreign Policy Imperative in the Digital Age," (Center for a New American Security, May 2011), https://www.cnas.org/publications/reports/internet-freedom-a-foreign-policy-imperative-in-the-digital-age.

38. Boutheina Guermazi and Natasha Beschorner, "Southeast Asia can Build a Stronger Digital Economy for all its Citizens," World Bank Group, June 25, 2019, https://blogs.worldbank.org/eastasiapacific/southeast-asia-can-build-stronger-digital-economy-all-its-citizens.

Center for a New American Security
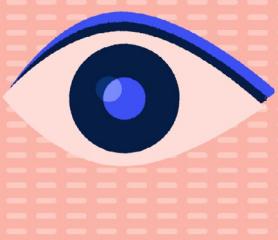
BLUNTING CHINA'S
AUTHORITARIAN
TOOLKIT

hosts its annual Global Startup Workshop in an emerging market country—to offer vocational training programs in coding, business administration, and other technical programs to support local entrepreneurs.[39]

9. **Raise the profile of the Indo-Pacific Transparency Initiative.** The U.S. government should strengthen awareness about the Indo-Pacific Transparency Initiative, concentrating its efforts in populous democratic countries that enjoy a relatively free information environment, such as the Philippines, Indonesia, and Malaysia.[40] It could, for example, appoint celebrity social media influencers as "digital ambassadors" who would travel to these countries and speak about the merits of using American social media platforms and living in an open society more broadly. U.S. ambassadors should also adopt more creative and aggressive social media strategies on American platforms to publicize and explain the activities of the Indo-Pacific Transparency Initiative and signal U.S. commitment to the free flow of information in open societies.

CONCLUSION

The openness of American social media platforms and the broader U.S. information environment is a vital asset, particularly when contrasted with the CCP's tightening chokehold on its domestic information space.[41] But as Chinese technology and social media companies gain a foothold in democracies around the world, these societies face a growing risk that Beijing will seek to shape their domestic information environment to advance its geopolitical ambitions.[42] The beginning and end of U.S. efforts to promote resilience, both at home and abroad, should, therefore, be to equip publics with a precise understanding of how Beijing is using popular platforms to censor, surveil, and erode truth amid its informational contest with the United States.

Center for a
New American
Security

39. MIT Global Startup Workshop 2018, Massachusetts Institute of Technology, March 2018, http://gsw.mit.edu/2018/.

40. "Freedom on the Net 2018." Freedom House. October 2018, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

41. Ely Ratner, Daniel Kliman, et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," forthcoming CNAS report, (Center for a New American Security, January 2020).

42. Patrick Cronin, Abigail Grace, Daniel Kliman, and Kristine Lee, "Contested Spaces: A Renewed Approach to Southeast Asia" (Center for a New American Security, March 2019), https://www.cnas.org/publications/reports/contested-spaces.