Defending U.S. Digital Dominance

Aditi Kumar

The geostrategic competition between the United States and China is heating up in the digital domain. Whereas American firms once dominated strategic markets from 4G to social media to payments, Chinese firms are gaining leadership in the next generation of these technologies. Increasingly, the U.S. is finding it necessary to play defense. In 2020, U.S. policy makers culminated a two-year global campaign against Huawei by inflicting crippling sanctions on the Chinese telecommunications provider. The Trump administration forced a partial sale of Chinese video-streaming app TikTok to American buyers under threat of an outright ban. An executive order has laid the groundwork to ban Chinese-owned payments and messaging app WeChat from American phones and app stores.

Huawei, TikTok, and WeChat are among the first Chinese tech companies to gain significant market share outside China, but they certainly won't be the last. More competitors are emerging, including some enabled by Xi Jinping's hallmark economic development strategy, "Made in China 2025," which aims to serve as a launchpad for critical technologies such as artificial intelligence, robotics, and biotechnology.[1]

However, the U.S. response thus far has been more akin to a game of whack-a-mole than a comprehensive strategy that recognizes and counters China's steadily increasing digital capabilities and ambitions. By restricting Chinese competition through sanctions, forced divestitures, bans, and other reactionary policies, the U.S. is doing little to address long-term national security risks emanating from how data on American citizens is collected, stored, and used by Chinese firms susceptible to government influence and control. At the same time, these policies are damaging American economic interests by creating an unpredictable business and investment environment, engaging China in a race-to-the-bottom tech trade war, and undercutting America's commitment to open and competitive markets.

The United States needs a strategy that protects both its national security and economic interests. To achieve these twin goals, policy makers must improve regulatory standards that all tech companies must follow as a condition for doing business in the United States; define clear policies and processes to identify, review, and mitigate national security threats; and build up domestic capabilities in technology markets that will be critical to American global strategic influence in the digital age.

A Shrinking Lead

The world is increasingly interconnected through digital platforms, devices, and telecommunication services that enable the global flows of information, goods, and money. Today, over 4.5 billion people, or 60 percent of the global population, are connected to the internet, spending an average of nearly seven hours online each day.[2] One of every two people in the world is an active social media user.[3] One of four is expected to buy goods and services online in 2020, contributing to retail e-commerce sales of $4.2 trillion.[4] The value of digital payments has more than doubled in the last three years, reaching $4.9 trillion in 2020, and is expected to double again by 2024.[5]

While American firms still top most digital league tables, China is positioning itself as a technological powerhouse to challenge U.S. primacy. The highest rates of mobile phone penetration and the largest internet user base in the world create a welcome digital ecosystem; thriving entrepreneurism and venture capital funding allow for the emergence of new digital business models; and a large and digital-savvy consumer base provides opportunities for rapid, large-scale

commercialization. Underpinning these advantages is an aggressive industrial policy that aims to make China a global leader in next-generation communications technology, advanced robotics, artificial intelligence, and other high-value sectors.[6] The program is accelerating digital advances by coordinating efforts across government, companies, and academia; deploying direct government subsidies to target sectors, including through state-owned enterprises; encouraging Chinese investment in foreign companies; and forcing technology transfers from foreign firms seeking access to China's expansive market.[7]

These concerted efforts to achieve global digital dominance are yielding results. Led by tech giants Alibaba and Tencent, China counts thirteen digital companies among the world's top 100 (based on a composite of financial metrics), the second highest number behind the U.S.[8] In 2019, China surpassed the U.S. in terms of the number of "unicorns," privately held startups valued at more than $1 billion, with digital payments provider Ant Financial and app platform (and TikTok parent) ByteDance topping the list.[9] In 2020, China became the first major economy to pilot a state-backed digital currency, with ambitions to transition most domestic transactions to the digital yuan by 2022.

While the size of the captive domestic market alone is enough to guarantee Chinese companies top global standings, it is their recent forays into foreign markets that truly herald the emergence of China as a global tech power—and competitor to U.S. primacy in key markets. For now, the ten digital platforms most visited by Americans are all U.S.-owned, topped by Google, Microsoft, Facebook, and Amazon.[10] But Chinese companies are starting to make inroads. TikTok reportedly hosts 50 million daily active users in the U.S., an eight-fold increase in just two years,[11] and WeChat hosts 19 million.[12] While limited in its penetration of U.S. markets, Huawei became the leading global provider of both 5G telecommunications equipment[13] and smartphones[14] in 2020.

China is further magnifying its global tech footprint through strategic investments in foreign firms. Chinese acquisitions and direct investments in U.S. companies grew from $10 billion in 2014 to a peak of $45 billion in 2016, primarily targeting the biopharma and telecommunications sectors. Chinese venture capital investments in the U.S. grew from $1 billion in 2014 to a peak of $4.7 billion in 2018, with the greatest increases in life sciences, blockchain, and fintech.[15]

Rising National Security Risks

The growing reach of China's tech tools and investments has given rise to a significantly more protectionist U.S. policy approach in domestic tech markets. Rather than reciprocating China's anti-competitive behavior, however, recent U.S. actions have been predicated on defending American citizens against Chinese-government surveillance, propaganda, and censorship.

At the root of policy makers' concerns are a patchwork of Chinese national security, intelligence, and cybersecurity laws that compel firms to respond to the government's request for data.[16] TikTok, for example, is at minimum tracking within-app user posts, messages, and browsing preferences and history. However, the company's privacy policy enumerates that it also collects users' IP address, geolocation data, unique device identifiers, cookies, and browsing and search history external to the platform.[17] President Trump's recent executive order banning TikTok states, "This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[18] Another risk is that Chinese companies will be used as avenues for state-sponsored propaganda, censorship, and disinformation campaigns. In the executive orders banning TikTok and WeChat, administration officials cite the censorship of content related to protests in Hong Kong and China's treatment of Uighurs and other Muslim minorities, as well as disinformation campaigns about the origins of the 2019 novel coronavirus.[19]

Over the longer term, the prevalence of Chinese tech tools and infrastructure in strategic global networks could increase China's capacity to coerce or challenge the United States and its allies. The U.S. has historically been at the helm of these networks, such as SWIFT and the dollar clearing system that routes the majority of global financial

transactions and gives the U.S. immense power to wield economic sanctions and track illicit financial flows around the globe. If Huawei emerges as the leader in 5G, for example, the Chinese government could realize similar advantages in the telecommunications network, exploiting its access to Huawei to have a "back door" to global communications.[20]

America's response to these policy threats has been reactionary and defensive. In the case of Huawei, the U.S. first banned American manufacturers from supplying the company with essential semiconductors, then expanded the ban to semiconductor manufacturers that use any American equipment—virtually all of them. Huawei joins a rapidly growing list of blacklisted entities, currently numbering over 1,400, that are restricted from using U.S.-origin technology and components without a license. The list was significantly expanded in 2019 and 2020, with the addition of over 400 entities predominantly based in China.[21]

Another powerful weapon in policy makers' arsenal is the little-known Committee on Foreign Investment in the U.S. (CFIUS). Composed of the heads of Treasury, Defense, State, and numerous other agencies, CFIUS scrutinizes foreign investments with an aim to balance national security, economic, and other concerns. Its recommendations can lead to blocking investments that are deemed a threat to national security or, as in the case of TikTok, unwinding transactions already completed (TikTok was investigated based on its merger with U.S.-headquartered app Musical.ly in 2017). In 2019, CFIUS reviewed 325 deals and investigated 113, a five-fold increase from a decade earlier. A rapidly evolving and expanding mandate, and the lack of clear guidelines on which investments merit a review, lead to a largely ad hoc selection process in which some companies self-nominate, while CFIUS can also initiate reviews on its own. To date, only five transactions have been formally blocked through this process, though this number certainly understates the Committee's true impact, as many others have been subject to stringent mitigation actions, as in the forced partial divestiture of TikTok to American buyers, or withdrawn entirely due to the threat of such actions. CFIUS does not disclose which deals are under review, the criteria or findings of its review, or required mitigation actions.[22]

The national security risks posed by Chinese tech are real and growing. However, banning or restricting companies on a one-off basis is neither a sustainable strategy, nor an effective one when it comes to safeguarding American economic and security interests. For one, an opaque and ad hoc process for blacklisting companies and blocking or imposing mitigation actions on foreign investments threatens to compromise the U.S.'s secure and predictable business environment, a pillar of American economic strength. Combined with the involvement of senior political appointees in key decisions, these actions can appear politically motivated and create even greater uncertainty. The impending partial sale of TikTok to an American firm led by a supporter of the president, for example, has already led to accusations of crony capitalism.[23]

Further, by imposing protectionist measures on Chinese firms, the U.S risks escalating the tech trade war with China. Following the executive order banning WeChat, China announced a new corporate blacklist, suggesting that American companies, including Apple and Google, would be prohibited from investing in China or trading with the Chinese market.[24] American semiconductor manufacturers have argued that restricting the export of American inputs to Huawei will simply shift this business elsewhere, and disadvantage American firms even more in the long term as R&D budgets are squeezed and China prioritizes building native capabilities.[25] China may already limit market access to U.S. firms, but there's plenty of runway for a race to the bottom. Qualcomm, Intel, and Apple rely on the Chinese market for 45, 28, and 15 percent of their revenue, respectively, and many of the largest American tech firms have built operations and deployed billions of assets in China.[26] An accelerated economic decoupling between the two countries would impose substantial costs on these firms.

Finally, beyond an even more frayed relationship with China, these policies undermine America's fair market principles and its commitment, as outlined in the 2017 National Security Strategy, "to advocate for open, interoperable communications, with minimal barriers to the global exchange of information and services."[27] By following China's lead in banning tech companies, forcing joint ventures, and restricting investment, the U.S. will lose credibility as the global champion of free markets. More countries may follow with digital controls based on protectionist aims, which will ultimately be the most hurtful to American tech giants.

Protecting America's Security and Economic Interests

In light of rising Chinese technological power, the United States must develop a comprehensive strategy that protects its national security objectives while enabling an open and competitive digital marketplace.

If the primary national security concerns relate to how companies collect, share, store, and use data on Americans, then policy makers should impose national data privacy and security standards that are uniformly applied to all firms as a condition of doing business in the United States. These standards should, among other requirements, compel companies to submit for regulatory review frequent audits of data collection practices, internal controls determining which employees and teams can access user data, cybersecurity plans, and content selection and moderation policies. And American companies should be held to these standards too, given the very real national security threats that have emanated from data breaches, data leaks, and rampant misinformation and disinformation campaigns on American platforms. Only once the U.S. has devised a domestic data privacy and security regime can it take a leading role in setting global standards that protect users.

Moreover, U.S. policy makers should outline a clear process and guidelines for how national security risks are identified, reviewed, and mitigated. Rather than relying on the ad hoc CFIUS self-nomination process, policy makers should specify criteria—for example, the types of data collected, the minimum number of active American users, and the minimum level of foreign investment—that would qualify a transaction for further review. Rather than opaque mitigation actions that allow certain deals to proceed while others are blocked, policy makers should make public the types of actions that companies can take to be allowed to operate in the United States.

Finally, policy makers cannot rely solely on mitigating the risks presented by Chinese tech firms; they must also adopt an offensive strategy that seeks to establish U.S. primacy in strategic digital markets and networks. This includes implementing measures outlined in the recent "National Strategy to Secure 5G," such as working with allies and partners to develop international 5G security principles and adopting policies to foster a competitive market of 5G vendors.[28] Policy makers must also seek to identify and invest early in new frontiers of technological competition, such as digital currencies and payments networks. Finally, they must ensure that the U.S. remains the destination for top technical talent through open immigration policies, robust STEM curricula, and affordable higher education and technical training programs.

Aditi Kumar is the Executive Director of the Belfer Center for Science and International Affairs at the Harvard Kennedy School, where she leads the Economic Diplomacy Initiative. Her research interests include U.S. international economic policy, financial technology, and financial regulation. Ms. Kumar was previously a principal at management consultancy Oliver Wyman in the financial services and public policy practices. She worked primarily with U.S. commercial and investment banks as well as U.S. regulators and policymakers on designing and implementing financial regulation. Ms. Kumar also served as a project manager at the World Economic Forum, responsible for leading policy discussions among financial sector executives and policymakers on managing financial risk and designing effective global financial regulation. She has undergraduate degrees in Finance and International Studies from the University of Pennsylvania, an M.B.A. from the Harvard Business School, and a master's degree in Public Policy from the Harvard Kennedy School.

[1] "Made in China 2025," State Council, July 7, 2015, http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf.

[2] Simon Kemp, "Digital 2020: 3.8 Billion People Use Social Media," We Are Social, January 30, 2020, https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.

[3] Ibid.

[4] "Number of Digital Buyers Worldwide from 2014 to 2021," Statista, accessed October 1, 2020, https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/; "Retail E-Commerce Sales Worldwide from 2014 to 2023," Statista, accessed October 1, 2020, https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

[5] "Digital Payments," Statista, accessed October 1, 2020, https://www.statista.com/outlook/296/100/digital-payments/worldwide.

[6] "'Made in China 2025' Plan Issued," The People's Republic of China, The State Council, May 19, 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

[7] James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

[8] "Greater China Ranks No. 2 on New Forbes Digital 100 List," *Forbes*, October 10, 2019, https://www.forbes.com/sites/forbeschina/2019/10/10/greater-china-ranks-no-2-on-new-forbes-digital-100-list/#5e2863866fae.

[9] "China Has More 'Unicorn' Start-Ups Than the U.S.," *BBC*, October 22, 2019, https://www.bbc.com/news/business-50134460.

[10] "Most Popular Multi-Platform Web Properties in the United States in July 2020, Based on Number of Unique Visitors," Statista, accessed October 1, 2020, https://www.statista.com/statistics/271412/most-visited-us-web-properties-based-on-number-of-visitors/.

[11] Alex Sherman, "TikTok Reveals Detailed User Numbers for the First Time," *CNBC*, August 24, 2020, https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html.

[12] Krystal Hu, "WeChat U.S. Ban Cuts off Users Link to Families in China," *Reuters*, August 7, 2020, https://www.reuters.com/article/us-usa-tencent-holdings-wechat-ban/wechat-u-s-ban-cuts-off-users-link-to-families-in-china-idUSKCN253339.

[13] "Mobile Base Station Vendor Market Share Worldwide in 2019 and 2020," Statista, accessed October 1, 2020, https://www.statista.com/statistics/1134472/global-mobile-base-station-vendor-market-share/.

[14] S. O'Dea, "Global Smartphone Market Share from 4th Quarter 2009 to 2nd Quarter 2020 (By Vendor)," Statista, August 20, 2020, https://www.statista.com/statistics/271496/global-market-share-held-by-smartphone-vendors-since-4th-quarter-2009/.

[15] "Pandemic and Politics: U.S.-China Investment Hits 9-Year Low," The U.S-China Investment Project, Rhodium Group, 2020, https://arraysproduction-0dot22.s3.amazonaws.com/rhodiumgroup/assets/icon/RHG_TWS-1H-2020-Report_16Sept2020.pdf.

[16] Samm Sacks, "Data Security and U.S.-China Tech Entanglement", *Lawfare*, April 2, 2020, https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement.

[17] "Privacy Policy," TikTok, January 1, 2020, https://www.tiktok.com/legal/privacy-policy?lang=en.

[18] Exec. Order No. 13942, 3 C.F.R. (2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

[19] Exec. Order No. 13943, 3 C.F.R. (2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

[20] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, No. 1 (Summer 2019): 42–79, doi.org/10.1162/ISEC_a_00351.

[21] "Consolidated Screening List," International Trade Administration, accessed October 1, 2020, https://www.trade.gov/consolidated-screening-list.

[22] "Annual Report to Congress," Department of the Treasury, Committee on Foreign Investment in the United States, 2019, https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.

[23] "Trump, TikTok and Crony Capitalism," *The Wall Street Journal,* September 20, 2020, https://www.wsj.com/articles/trump-tiktok-and-crony-capitalism-11600639766.

[24] Gerry Shih, "China Threatens U.S. Companies with Sanctions Following Trump's WeChat Ban," *The Washington Post,* September 19, 2020, https://www.washingtonpost.com/world/china-threatens-us-companies-with-sanctions-following-trumps-wechat-ban/2020/09/19/08c4a0d8-fa55-11ea-89e3-4b9efa36dc64_story.html.

[25] Aime Williams, "Why Washington's Clampdown on Chinese Chipmakers Could Backfire," *Financial Times,* September 30, 2020, https://www.ft.com/content/e1f20f9e-ada1-4942-a83b-92b4a4f4e49b.

[26] "Pandemic and Politics: U.S.-China Investment Hits 9-Year Low," The U.S-China Investment Project, Rhodium Group, 2020, https://arraysproduction-0dot22.s3.amazonaws.com/rhodiumgroup/assets/icon/RHG_TWS-1H-2020-Report_16Sept2020.pdf.

[27] "National Security Strategy," The White House, 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[28] "National Strategy to Secure 5G of the United States of America," The White House, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.