Beyond Huawei and TikTok: Untangling U.S. Concerns over Chinese Tech Companies and Digital Security

Robert D. Williams
Executive Director, Paul Tsai China Center, Yale Law School

Washington's growing focus on the risks posed by Chinese technology companies operating in the United States embodies the complexity of the challenges confronting U.S. policymakers in responding to China's rise in technological, economic, and geopolitical power. Concerns over companies such as telecommunications equipment-maker Huawei and social-media platform TikTok are multidimensional and scarcely amenable to characterization in terms of discrete national security risks.

This paper traces one aspect of the "securitization" of technology policy in U.S.-China relations. It seeks to identify and disaggregate the main challenges facing policymakers who are troubled by China's growing technological power as expressed through the actual or potential effects of Chinese technology companies doing business in the U.S. market. These concerns can be broadly categorized along (at least) two dimensions: risks inherent in the nature of emerging technologies and risks related to the nature of China's governing system. The paper illustrates how these concerns apply in the context of 5G telecommunications and artificial intelligence.

The essay concludes with several recommendations for U.S. policy reform: (1) enacting comprehensive federal data privacy legislation; (2) advancing a digital trade agenda with U.S. allies and partners; (3) rationalizing the U.S. cybersecurity liability regime; (4) increasing the costs for malicious hackers; and (5) improving mechanisms for governmental policy coordination along domestic and international dimensions.

Chinese telecommunications giant Huawei has become an avatar for (and target of) a range of U.S. government concerns about the ways China might choose to wield its considerable technological, economic, political, and military power. But Huawei is far from alone. Washington's growing focus on the risks posed by Chinese technology companies operating in the United States embodies a central challenge confronting the stewards of American security and prosperity—the preservation of which is increasingly viewed as hinging on the United States'

response to China's rise.[1] Concerns over companies such as Huawei and social-media platform TikTok are multidimensional and scarcely amenable to characterization in terms of discrete national security risks. Similarly, the tools U.S. policymakers are increasingly employing to address these risks—from export controls to foreign investment reviews to outright bans on certain companies—do not fully capture the subtleties of the challenges at hand.

This paper traces one aspect of the "securitization" of technology policy in U.S.-China relations. It seeks to identify and disaggregate the main challenges facing policymakers who are troubled by China's growing technological power as expressed through the actual or potential effects of Chinese technology companies doing business in the U.S. market. Their concerns can be broadly categorized along (at least) two dimensions: (1) risks inherent in the nature of emerging technologies, and (2) risks related to the nature of China's governing system. I seek to illustrate how these concerns apply in the context of 5G telecommunications and artificial intelligence. The essay concludes with several recommendations for U.S. policy reform.

Technological Risks

A fundamental security challenge with new technologies is what might be called the "omni-use problem." Technologies such as fifth-generation (5G) telecommunications networks, artificial intelligence (AI), quantum computing, and semiconductors have inherently dual-use (civilian and military) applications. Moreover, they underpin and serve as building blocks for many applications or end-use technologies to be built upon them.[2] Their pervasiveness and

[1] *See* National Security Strategy of the United States of America, White House (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[2] *See* Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, Defense Innovation Unit Experimental (DIUx) (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; Brigitte Dekker & Maaike Okano-Heijmans, *The US–China trade–tech stand-off and the need for EU action on export control*, Clingendael Report (Aug. 2019), https://www.clingendael.org/sites/default/files/2019-08/Report_US-China_stand-off.pdf

growing importance to the functioning of national economies and defense institutions blurs the lines between economic and national security interests. Below I outline some of the technological features that contribute to this state of affairs in 5G and AI.

5G Networks

The fifth generation of cellular network technology promises to deliver a step change in mobile communications with faster download speeds, lower latency (the delay in sending and receiving data), and capacity to handle many more connected devices.[3] 5G networks will be significantly more complex than previous generations, which were designed primarily for consumer voice and data services. These networks will support at least three major functions: (1) enhanced mobile broadband, which will enable faster download speeds for consumers; (2) ultra-reliable low-latency communication, designed for autonomous vehicles and other applications requiring no gaps in communication; and (3) massive machine-to-machine communications, or the Internet of Things (IoT).[4]

Prior generations of mobile technology involved devices connecting to the network in a hub-and-spoke architecture with centralized, hardware-based switching. In 5G, billions of IoT devices will connect with one another in a web-like environment with distributed, software-defined digital routing.[5] There is some debate about the extent to which these features of 5G blur or collapse the traditional distinction between the so-called "core" telecom network, where more

("[E]merging technologies are integrated at all levels of society, especially amid the increasing convergence of software and information flows, making them also omnipresent in society. One can therefore speak about the 'omni-use' of those technologies rather than a clear dual-use, whereby most countries agree on the potential civilian and military purposes of an item."); Elsa Kania, *The Dual-Use Dilemma in China's New AI Plan: Leveraging Foreign Innovation Resources and Military-Civil Fusion*, Lawfare (July 28, 2017), https://www.lawfareblog.com/dual-use-dilemma-chinas-new-ai-plan-leveraging-foreign-innovation-resources-and-military-civil.

[3] Will Knight, *The White House Announces a Plan to Speed the Rollout of 5G*, Wired (Aug. 10, 2020), https://www.wired.com/story/white-house-plan-speed-rollout-5g/.

[4] *See, e.g.*, Adrian Jakobsson, *The 5G Future Will Be Powered By AI*, Network Computing (Mar. 14, 2019), https://www.networkcomputing.com/wireless-infrastructure/5g-future-will-be-powered-ai; Paul Triolo & Kevin Allison, *The Geopolitics of 5G*, Eurasia Group (Nov. 15, 2018), https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g.

[5] Tom Wheeler & David Simpson, *Why 5G requires new approaches to cybersecurity*, Brookings Inst. (Sept. 3, 2019), https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

sensitive functions such as central switching and data authentication occur, and the "edge" of the network, where user devices connect to small-cell radio units (known as the radio access network, or RAN).[6] Few would dispute, however, that the security implications of these changes are considerable.[7]

For example, in traditional networks, "everything came to hardware choke points where cyber hygiene could be practiced. In the 5G software-defined network, however, that activity is pushed outward to a web of digital routers throughout the network, thus denying the potential for choke point inspection and control."[8] Vulnerabilities in the AI-driven software managing the network could be exploited by malicious hackers; the same can happen to connected devices themselves. The web-like architecture of IoT devices dramatically expands the opportunities for, and consequences of, such cyberattacks.[9]

5G network infrastructure can accurately be described as critical infrastructure.[10] These networks will undergird a variety of critical functions, including autonomous vehicles, smart electric grids, intelligent medicine, and military communications. As companies and individuals become increasingly dependent on these networks, they become more vulnerable to the theft of sensitive data traversing the network, attacks on and disruptions of the functioning of connected devices by other devices, and attacks that disrupt or degrade the network itself. 5G networks will

[6] *See* Justin Sherman, *Making Sense of a Huawei "Partial Ban"*, New America (July 3, 2019), https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/making-sense-huawei-partial-ban/. This functionality may depend to some extent on geographic factors that vary across jurisdictions.

[7] *See* Triolo & Allison, *supra* note 4; Ian Levy, *Security, complexity and Huawei; protecting the UK's telecoms networks*, UK National Cyber Security Centre (Feb. 22, 2019), https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks; Wheeler & Simpson, *supra* note 5.

[8] Wheeler & Simpson, *supra* note 5. For example, secret portals known as "backdoors" could be installed in mobile base stations, enabling data interception or manipulation from one of the numerous access points in the RAN. *See* Nicolas Botton & Hosuk Lee-Makiyama, *5G and National Security: After Australia's Telecom Sector Security Review*, Eur. Ctr. Int'l & Pol. Econ. (Oct. 2018), https://ecipe.org/publications/5g-national-security-australias-telecom-sector/.

[9] *See* Robert D. Williams, *Securing 5G Networks: Challenges and Recommendations*, Council on Foreign Rel. (July 15, 2019), https://www.cfr.org/report/securing-5g-networks.

[10] *See CISA 5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation*, U.S. Dep't of Homeland Sec., Cybersecurity and Infrastructure Sec. Agency (Aug. 2020), https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf; *National Critical Functions Set*, U.S. Dep't of Homeland Sec., Cybersecurity and Infrastructure Security Agency (revised May 13, 2020), https://www.cisa.gov/national-critical-functions-set.

expand the number and scale of potential vulnerabilities, increase incentives for malicious actors to exploit those vulnerabilities, and potentially make it more difficult to detect malicious cyber activity.[11]

In sum, 5G networks manifest the omni-use problem on at least two levels. First, these networks will be utilized by the commercial and governmental sectors, providing a foundation for private commercial activities and for military and intelligence services alike. Second, the economic considerations raised by 5G networks may rise to the level of national security considerations in the sense that entire economies will be dependent on their smooth functioning as a component of critical infrastructure. Individually and collectively, these attributes heighten the concerns of policymakers about the possibility that an adversary foreign government or malicious cyber actor could exploit 5G infrastructure for espionage or sabotage against the United States.[12]

Artificial Intelligence

Artificial intelligence (AI) is not a singular technology but rather a "tool with innumerable uses."[13] Although there is no commonly accepted definition of AI, a recent report by the National Security Commission on Artificial Intelligence (NSCAI) characterizes it thus:

> AI is the ability of a computer system to solve problems and to perform tasks that would otherwise require human intelligence. AI technologies have evolved for many decades, including pattern recognition, machine learning, computer vision, natural language understanding, and speech recognition. These technologies are harnessed to enhance the abilities of both humans and machines, helping them to make decisions of higher quality and at greater speed.[14]

---

[11] Williams, *supra* note 9.
[12] *See generally* National Strategy to Secure 5G of the United States of America, White House (Mar. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf. *See also* Tom Wheeler & Robert D. Williams, *Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G*, Lawfare (Feb. 20, 2019), https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g.
[13] R. David Edelman, *Here's how to regulate artificial intelligence properly*, Wash. Post (Jan. 13, 2020), https://www.washingtonpost.com/outlook/2020/01/13/heres-how-regulate-artificial-intelligence-properly/.
[14] National Security Commission on Artificial Intelligence: Interim Report for Congress (Nov. 2019), https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view.

Although machine-learning AI—that is, systems that generate their own rules from training data rather than being explicitly programmed by humans—has been around for decades, its practical salience and significance has grown dramatically due to several factors. These include recent increases in the availability of massive datasets, improvements in computing power, more robust and flexible algorithms, and the availability of open source-code libraries and technical frameworks that allow developers to leverage the work of others for new use cases.[15]

Setting aside the prospects of developing "artificial general intelligence," the national security implications of AI, even narrowly defined, become apparent when considering its role as an enabling technology akin to electricity.[16] For example, AI has numerous potential applications in the field of intelligence, surveillance, and reconnaissance. Computer vision and machine learning algorithms that support social networking or manufacturing can also be deployed to instantaneously review footage from remotely piloted aircraft and identify and track targets of military or intelligence value. Software that enables image and speech recognition, predictive analytics, geolocation from image metadata, and pattern-of-life analysis can offer enormous potential benefits for the missions of militaries and security services.[17] Cyber operations increasingly call for the use of AI for both defensive and offensive purposes—for example, to automate the tasks of detecting and patching (or exploiting) vulnerabilities.[18] Similar concepts apply in the context of military logistics and command-and-control systems, where predictive

[15] Greg Allen, *Understanding AI Technology*, DoD Joint AI Center (Apr. 2020), https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.
[16] Michael C. Horowitz, *Artificial Intelligence, International Competition, and the Balance of Power*, 1 Tex. Nat'l Sec. Rev. 37 (May 2018), https://repositories.lib.utexas.edu/bitstream/handle/2152/65638/TNSR-Vol-1-Iss-3_Horowitz.pdf?sequence=2&isAllowed=y.
[17] Kelley M. Sayler, *Artificial Intelligence and National Security*, Cong. Res. Serv. (Aug. 26, 2020), https://fas.org/sgp/crs/natsec/R45178.pdf.
[18] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Oxford Future of Humanity Inst. (Feb. 2018), https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/1c6q2kc4v_50335.pdf.

analytics and integration of data from multiple sensors can facilitate enormous time and cost efficiencies that afford tactical and strategic advantages against adversaries.[19]

Moreover, AI systems themselves also present novel vulnerabilities that could constitute national security threats. Among these are "data poisoning attacks (introducing training data that causes a learning system to make mistakes), adversarial examples (inputs designed to be misclassified by machine learning systems), and the exploitation of flaws in the design of autonomous systems' goals."[20] To the extent AI systems assist in performing critical national functions such as cyber defense of government computer systems, military targeting, or command-and-control, these potential vulnerabilities are not merely risks—they are national security risks.

In short, AI is an amorphous concept that refers not to a single technology but to a range of enabling technologies that are inherently dual-use.[21] According to an influential 2018 report by the Defense Innovation Unit Experimental (DIUx), at present, "the U.S. government is actively making investments to create the third wave of AI technology to achieve a future where machines can explain themselves to humans; where machines can create causal models, not just correlations; and where machines can take what they learn in one domain and apply the learnings to a completely different domain."[22] Yet most advances in AI development are being driven by the commercial sector, not by governments.[23] The task of partitioning the potential commercial applications of these capabilities from noncommercial and national security-related applications is extremely difficult.

[19] Brundage et al. at 10-11.
[20] *Id.* at 17-18 (internal citations omitted).
[21] Robert D. Williams, *In the Balance: The Future of America's National Security and Innovation Ecosystem*, Lawfare (Nov. 30, 2018), https://www.lawfareblog.com/balance-future-americas-national-security-and-innovation-ecosystem.
[22] Brown & Singh, *supra* note 2, at 8.
[23] *See* Sayler, *supra* note 17, at 16.

Data Security as National Security

The foregoing examples of 5G telecommunications networks and artificial intelligence are intended to be illustrative of technologies that exhibit the omni-use problem, not an exhaustive list.[24] They are useful examples, however, because they are linked by a common thread: data.

Data is the lifeblood of a telecommunications system—the constituent elements that transit the system, sustain the system, and enable the economic and security architecture built upon the system. Data is similarly a key ingredient in the development of AI. As Randy Bean has written, "Although many AI technologies have been in existence for several decades, only now are they able to take advantage of datasets of sufficient size to provide meaningful learning and results. The ability to access large volumes of data with agility and ready access is leading to a rapid evolution in the application of AI and machine-learning applications."[25] No wonder, then, that data is sometimes described as a strategic resource.[26]

Structural concerns around the uses to which data can be put are accentuated by specific anxieties regarding the security implications of certain types of data, particularly personally identifiable information. Fueled by years of reports that China's government is building a massive database on American citizens, experts fear U.S. citizen information could be used to develop a mosaic picture of users' lives and habits, creating (among other things) opportunities

[24] Other examples include semiconductors and biotechnology. *See, e.g.*, Saif M. Khan & Carrick Flynn, *Maintaining China's Dependence on Democracies for Advanced Computer Chips*, Brookings Inst. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_computer_chips_khan_flynn.pdf ; Scott Moore, *China's Role in the Global Biotechnology Sector and Implications for U.S. Policy*, Brookings Inst. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_biotechnology_moore.pdf.

[25] Randy Bean, *How Big Data is Empowering AI and Machine Learning at Scale*, MIT Sloan Mgmt. Rev. (May 08, 2017), https://sloanreview.mit.edu/article/how-big-data-is-empowering-ai-and-machine-learning-at-scale/.

[26] Justin Sherman & Samm Sacks, *The Myth of China's Big A.I. Advantage*, Slate (June 13, 2019), https://slate.com/technology/2019/06/data-not-new-oil-kai-fu-lee-china-artificial-intelligence.html.

to blackmail those with actual or potential access to sensitive national security information.[27] Notable personal-data breaches involving Chinese hackers include the Office of Personnel Management hack that exposed security-clearance records and sensitive information on 22 million Americans,[28] the pilfering of data on nearly 80 million customers from health insurer Anthem,[29] the breach of Marriott that compromised data on 500 million guests of "the top hotel provider for American government and military personnel,"[30] and the cybertheft of sensitive information on 147 million Americans from credit-reporting agency Equifax.[31] The U.S. government is increasingly treating this personal data as a dual-use item with both commercial and national-security value. As Attorney General William Barr said of the alleged theft of Equifax customer data by members of China's People's Liberation Army (PLA), "This data has economic value, and these thefts can feed China's development of artificial intelligence tools as well as the creation of intelligence targeting packages."[32]

To be sure, the ecosystem required to develop AI is much broader and more complex than mere data aggregation. Factors contributing to AI development include "a skilled and knowledgeable workforce; a digital infrastructure for capturing, handling and exploiting data; a technical foundation of trust, security and reliability; and an investment environment and

[27] *See, e.g.*, Eric Tucker & Michael Balsamo, *US says Chinese military stole masses of Americans' data*, Assoc. Press (Feb. 10, 2020), https://apnews.com/05aa58325be0a85d44c637bd891e668f; Ellen Nakashima, *With a series of major hacks, China builds a database on Americans*, Wash. Post (June 5, 2015), https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html; Preston Hogue, *The Risk of Triangulation: You May Just be a Piece of the Puzzle*, Sec. Week (Sept. 11, 2018), https://www.securityweek.com/risk-triangulation-you-may-just-be-piece-puzzle.

[28] Ellen Nakashima, *Hacks of OPM databases Compromised 22.1 million people, Federal Authorities Say*, Wash. Post (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[29] Dustin Volz, *Chinese National Indicted on Hacking Charges related to Anthem Breach*, Wall St. J. (May 9, 2019), https://www.wsj.com/articles/chinese-national-indicted-on-hacking-charges-related-to-anthem-breach-11557433541.

[30] David E. Sanger et al., *Marriott Data Breach is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. Times (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[31] *See* Robert D. Williams, *America's Hopelessly Anemic Response to One of the Largest Personal-Data Breaches Ever*, Atlantic (Feb. 12, 2020), https://www.theatlantic.com/ideas/archive/2020/02/whats-behind-the-indictment-of-the-equifax-hackers/606466/.

[32] Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, U.S. Dep't of Justice (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

strategic policy framework that provides the top-cover and fuel for growth."[33] Ensuring U.S. national security through AI innovation cannot simply be a matter of controlling data-driven technologies; it requires ensuring an open economic, academic, and immigration climate that enables the free flow of data and ideas along with human and financial capital.[34]

I have referred to the challenge of striking the proper balance of openness and control, of data flows and data protection, as the "innovation-security conundrum."[35] The point for present purposes is not to attempt to resolve that puzzle. It is simply to observe that at a fundamental level, whether consciously or unconsciously in the minds of American officials, data security has become synonymous with national security.[36] This in turn has triggered fears about the extent to which Chinese companies operating in the United States might gain access to data on U.S. citizens or seek to exploit the relatively open U.S. data environment for purposes that may threaten national security, economic prosperity, and political values. These risks arise not only as a function of new technologies themselves—they are also informed by background concerns regarding China's governing system, to which we now turn.

Sources of Distrust

Chinese companies are increasingly leading the development and commercialization of cutting-edge technologies. Security, of a nation-state or otherwise, is not an on/off switch—it is

[33] Lindsey Sheppard, *AI is a national security priority – Here's how we cultivate it*, Hill (Feb. 20, 2019), https://thehill.com/opinion/cybersecurity/430765-ai-is-a-national-security-priority-heres-how-we-cultivate-it.
[34] *See* Williams, *supra* note 21.
[35] Robert D. Williams, *The Innovation-Security Conundrum in U.S.-China Relations*, Lawfare (July 24, 2018), https://www.lawfareblog.com/innovation-security-conundrum-us-china-relations. I will not attempt here to resolve definitional distinctions between terms such as "data security," "data privacy," and "cybersecurity." William McGeveran offers the following taxonomy: "*Data security* is just one element of the broader concept of *data privacy*; the latter also relates to the collection, use, and disclosure or personal data in addition to its secure storage. Data security is not quite the same thing as *cybersecurity* either. Data security protects the personal information held by an entity; cybersecurity protects the network's infrastructure." William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1141 (2019).
[36] Robert D. Williams, *Reflections on TikTok and Data Privacy as National Security*, Lawfare (Nov. 15, 2019), https://www.lawfareblog.com/reflections-tiktok-and-data-privacy-national-security. As discussed further *infra*, this is a striking shift that arguably moves the U.S. closer to viewpoints long reflected in the Chinese government.

more usefully conceived as a calibration of risk tolerance. In the United States, that tolerance is being tested in novel ways by the combination of China's technological prowess and its system of governance. Four categories of political concern stand out: China's strategic intentions, its structural economic policies, the absence of reliable legal checks on governmental power, and potential threats to human rights and liberal values. The following section examines these systemic issues through the lens of Chinese companies operating in the areas of 5G telecommunications and artificial intelligence.

Systemic Bases of Distrust

i. China's Statements of Strategic Aspiration

First, consider the problem of assessing Beijing's strategic intentions. The Chinese Communist Party (CCP) has made no secret of its ambition to transform China into a superpower in science and technology. That ambition, which dates to the origins of the People's Republic of China in 1949, is encapsulated by President Xi Jinping's references to pursuing an "asymmetric strategy" to "catch up and surpass"[37] and by his exhortations to reach for the "commanding heights" in science and technology.[38] These ideologically rooted objectives find policy direction in aspirational initiatives such as "Made in China 2025," an economic plan designed to increase China's technological competitiveness and move the country's manufactured goods up the value chain, in part by cutting China's reliance on foreign technological inputs.[39] The CCP's goals also find expression in the State Council's 2017 New Generation Artificial Intelligence Development Plan, which sets broad targets for AI policy and development, including the aspiration to make

[37] Julian Baird Gewirtz, *China's Long March to Technological Supremacy*, Foreign Aff. (Aug. 27, 2019), https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy.
[38] Ju Peng, *Xi Calls for Developing China into World Science and Technology Leader*, Xinhua (May 29, 2018), http://en.people.cn/n3/2018/0529/c90000-9464968.html.
[39] Jeremy Goldkorn et al., *Made in China 2025: The domestic tech plan that sparked an international backlash*, SupChina (June 28, 2018), https://supchina.com/2018/06/28/made-in-china-2025/.

China the world's "primary AI innovation center" by 2030.[40] Such plans emphasize the concept of "civil-military fusion," a longstanding effort to reduce barriers between China's private sector and military-industrial base.[41] China is also prioritizing the "Digital Silk Road" component of its Belt and Road global infrastructure initiative, which analysts have indicated "could emerge as a vehicle through which Beijing pushes for an alternative to what it sees as a U.S.-dominated technology world."[42]

Some of these high-level statements of aspiration are sufficient to arouse concern even in the absence of concrete policies to implement them. For example, the Ministry of Industry and Information Technology's "Key Technology Roadmap" to advance the goals of Made in China 2025 contains specific targets for Chinese tech companies to increase their market share in both the domestic and global markets.[43] By negative implication, this could be (and widely has been) interpreted as a national goal to *reduce* the market share of foreign companies in the cutting-edge sectors most important to economic growth. Foreign governments and business groups have viewed such statements as an explicit intention not to open China's market in fulfillment of hopes embedded in China's 2001 accession to the World Trade Organization (WTO), but instead to increasingly exclude foreign companies from it.[44] This perception is buttressed by the assessment that Beijing's ambitions are being driven by an expansive vision of national security,

[40] Graham Webster et al., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)*, New Am. (Aug. 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.
[41] Lorand Laskai, *Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise*, Council on Foreign Rel. (Jan. 29, 2018), https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise.
[42] Paul Triolo & Robert Greene, *Will China control the global internet via its Digital Silk Road?*, SupChina (May 8, 2020), https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/amp/.
[43] *Unofficial USCBC Chart of Localization Targets by Sector Set in the MIIT Made in China 2025 Key Technology Roadmap*, U.S.-China Bus. Council (Feb. 2016), https://www.uschina.org/sites/default/files/2-2-16%20Sector%20and%20Localization%20Targets%20for%20Made%20in%20China%202025.pdf.
[44] *See* James McBride & Andrew Chatzky, *Is 'Made in China 2025' a Threat to Global Trade?*, Council on Foreign Rel. (May 13, 2019), https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade; Michael Martina, *EU business group slams Beijing's 'Made in China' plan*, Reuters (Mar. 6, 2017), https://www.reuters.com/article/us-china-eu-business/eu-business-group-slams-beijings-made-in-china-plan-idUSKBN16E0A2.

according to which China's drive for technological self-sufficiency is partly a means to reduce the vulnerabilities that flow from interdependence with the United States.[45]

ii. Chinese Policies and Practices

Second, certain Chinese policies and activities—whether they are intended to further the goal of technological supremacy or simply inhere to China's state-led economic model—reinforce difficult questions about the extent to which China's approach to technological competition is compatible with U.S. interests.

Some policies are directly threatening, such as commercial espionage and cyber-enabled theft of intellectual property (IP) from U.S. companies.[46] Although measuring the scale of data breaches and IP theft is notoriously difficult and imprecise, the IP Commission estimates at the low end that the value of Chinese theft of American IP exceeds $225 billion annually.[47] Recent history suggests China has little intention to discontinue its campaign of state-sponsored hacking. In 2015, President Xi Jinping reached a landmark agreement with President Barack Obama that neither country would "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[48] In the years since that pledge, however, a raft of high-profile U.S. indictments against Chinese state-linked hackers indicates

[45] *See* Julian Gewirtz, *The Chinese Reassessment of Interdependence*, China Leadership Monitor (June 1, 2020), https://www.prcleader.org/gewirtz; Kristin Huang, *China must become self-reliant in key technology to be secure, says military newspaper*, S. China Morning Post (Oct. 6, 2020), https://www.scmp.com/news/china/military/article/3104367/china-must-become-self-reliant-key-technology-be-secure-says.

[46] *See* Robert D. Williams, *The 'China, Inc.+' Challenge to Cyberspace Norms*, Hoover Inst. (Feb. 2018), https://www.hoover.org/sites/default/files/research/docs/williams_webreadypdf1.pdf; Jack Goldsmith & Robert D. Williams, *The Chinese Hacking Indictments and the Frail "Norm" Against Commercial Espionage*, Lawfare (Nov. 30, 2017), https://www.lawfareblog.com/chinese-hacking-indictments-and-frail-norm-against-commercial-espionage.

[47] *See Update to the IP Commission Report – The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, Nat'l Bureau of Asian Res. (Feb. 2017), http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; *see also Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, Office of the U.S. Trade Rep. (Mar. 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF [hereinafter, "Section 301 Report"].

[48] *See Fact Sheet: President Xi Jinping's State Visit to the United States*, White House (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states; Williams, *supra* note 46.

that Beijing has either blatantly violated the 2015 agreement or exploited its ambiguities by continuing to countenance cyber-enabled industrial espionage on a massive scale.[49]

Beyond the realm of commercial cybertheft, the U.S. government is also increasingly attentive to the threat of state-sponsored hackers from China, Russia, and elsewhere placing malware in the digital networks that underpin the U.S. electric grid and other critical infrastructure.[50] Washington's growing focus on supply-chain security extends not only to hardware but also to software—a salient vector of concern given that 5G networks will be largely "software defined."[51] On September 16, 2020, the U.S. Department of Justice (DOJ) unsealed indictments against five Chinese nationals for conducting a massive hacking campaign against more than 100 victim companies globally, from social-media firms to telecom providers.[52] According to the Justice Department, the hackers "compromised software providers around the world, and modified the providers' code to install backdoors that enabled further hacks against the software providers' customers."[53] Although prosecutors did not directly allege that the hackers were supported by the Chinese government, DOJ accused the CCP of "making

[49] Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, Lawfare (Dec. 28, 2018), https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy; Williams, *supra* note 46; Dustin Volz, *China Violated Obama-Era Cybertheft Pact, U.S. Official Says*, Wall St. J. (Nov. 8, 2018), https://www.wsj.com/articles/china-violated-obama-era-cybertheft-pact-u-s-official-says-1541716952.

[50] Joyce Corell et al., *Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions*, Public-Private Analytic Exchange Program (2017), at 6, https://www.odni.gov/files/PE/Documents/11---Supply-Chain-Risks-of-SCADA-Industrial-Control-Systems-in-the-Electricity-Sector_Risks-and-Mitigations.pdf; Justin Sherman & Tanjiu Zuo, *Energy Grid Supply-Chain Risks and U.S.-China Entanglement*, Lawfare (June 8, 2020), https://www.lawfareblog.com/energy-grid-supply-chain-risks-and-us-china-entanglement; Constance Douris, *Cyber Threats to the U.S. Electric Grid Are Real*, Nat'l Int. (Jan. 9, 2017), https://nationalinterest.org/blog/the-buzz/cyber-threats-the-us-electric-grid-are-real-19000 ("U.S. officials have tracked efforts by China, Russia and other countries to implant malicious software inside computers used by U.S. utilities as far back as 2009.").

[51] *See, e.g.*, Wheeler & Simpson, *supra* note 5.

[52] Duston Volz et al., *U.S. Charges Chinese Nationals in Cyberattacks on More Than 100 Companies*, Wall St. J. (Sept. 16, 2020), https://www.wsj.com/articles/justice-department-unseals-indictments-alleging-chinese-hacking-against-u-s-international-firms-11600269024.

[53] Remarks by Deputy Attorney General Jeffrey A. Rosen at an Announcement of Charges and Arrests in Computer Intrusion Campaigns Related to China, U.S. Dep't of Justice (Sept. 16, 2020), https://www.justice.gov/opa/speech/remarks-deputy-attorney-general-jeffrey-rosen-announcement-charges-and-arrests-computer [hereinafter, "Rosen Remarks"].

China safe for their own cyber criminals, so long as they help with [the CCP's] goals of stealing intellectual property and stifling freedom."[54]

This is not to suggest that Chinese technology-acquisition policies are pervasively threatening. Many practices entail more benign forms of economic competition. These include the hiring of foreign experts, pursuit of joint ventures and partnerships, and outbound investment in early-stage technologies in fields such as artificial intelligence, robotics, and financial technology.[55]

Other policies exist in a complicated gray area of legality but are likely inconsistent with the spirit of China's obligations under WTO rules and contrary to principles of fair competition. This category includes restrictions on foreign companies' access to China's domestic market, such as joint venture requirements that result in "forced transfer" of technology from foreign to Chinese firms; discriminatory licensing and administrative requirements for foreign companies operating in China, some of which also result in forced tech transfer; and state-directed technology acquisition policies such as providing preferential access to capital for Chinese firms to engage in overseas acquisitions.[56] In addition, China's industrial subsidies to "national champion" companies in strategic sectors have raised hackles in Western capitals. Economist Nicholas Lardy estimates that "China now devotes more than 3 percent of its annual output to direct and indirect business subsidies—a share of the economy that is roughly equivalent to what the United States spends on defense."[57] The United States, European Union, and Japan argue that

[54] *Id.*
[55] *See* Brown & Singh, *supra* note 2.
[56] *See* Section 301 Report, *supra* note 47; *United States Strategic Approach to the People's Republic of China*, White House (May 2020), https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf.
[57] David J. Lynch, *Initial U.S.-China trade deal has major hole: Beijing's massive business subsidies*, Wash. Post (Dec. 31, 2019), https://www.washingtonpost.com/business/economy/initial-us-china-trade-deal-has-major-hole-beijings-massive-business-subsidies/2019/12/30/f4de4d14-22a3-11ea-86f3-3b5019d451db_story.html.

such subsidies create market distortions and make it difficult for foreign firms to compete in the global market.[58]

China's approach to domestic and international technical standards has further fueled complaints about fair competition.[59] According to a 2016 report by the Mercator Institute for China Studies (MERICS), "China sometimes formulates national standards in strategic industries that deliberately differ from international standards in order to impede market access for foreign technology and to favor Chinese technology on the domestic market."[60]

China's role in the process of setting international technical standards has raised similar worries. For example, Beijing has been accused of politicizing the process of setting 5G standards by creating an expectation that Chinese companies participating in the multi-stakeholder 3GPP (Third Generation Partnership Project) will vote for Chinese-proposed standards whether or not they are technically superior.[61] Like government subsidies, technical standards are primarily an economic rather than security issue, as "[c]ompanies whose technology becomes the industry standard for 5G will receive royalty payments from other ecosystem participants. Those payments, in turn, will help fund future innovation."[62] There is nothing unusual about companies vying to have their own patented technology incorporated into an agreed standard.[63] But to the extent there are independent security concerns around the companies engaged in standard-setting, the market advantages those companies gain through

[58] Philip Blenkinsop, *U.S., EU, Japan agree new subsidy rules with China trade in focus*, Reuters (Jan. 14, 2020), https://www.reuters.com/article/us-trade-wto-subsidies/us-eu-japan-agree-new-subsidy-rules-with-china-trade-in-focus-idUSKBN1ZD1RM.
[59] *See generally* John Seaman, *China and the New Geopolitics of Technical Standardization*, IFRI (Jan. 2020), https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.
[60] Jost Wübbeke et al., *Made in China 2025: The making of a high-tech superpower and consequences for industrial countries*, MERICS (Aug. 12, 2016), at 56, https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf (further noting that "[e]xamples of Chinese national standards are the FDD-LTE standard for 4G mobile networks, the WAPI standard for wireless networks and independent standards for electric vehicle charging stations.").
[61] *See* James A. Lewis, *How 5G Will Shape Innovation and Security: A Primer*, CSIS (Dec. 2018), at 7, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf.
[62] Triolo & Allison, *supra* note 4, at 8.
[63] Eli Greenbaum, *5G, Standard-Setting, and National Security*, Harv. Nat'l Sec. J. (July 3, 2018), https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/.

"standard essential patents" could become a structural security advantage as firms leverage the economic benefits of patent royalties to drive growth and expand their presence in overseas markets.[64]

iii. Party-State Governance

A third category of concern relates to the pervasive nature of CCP power in China's domestic economic and legal system. This is related to, but distinct from, the structural economic and standards-related policies noted above. The thrust of the worry is that even if Chinese technology companies *want* to be independent from the Chinese party-state, they operate within a legal and political framework that makes it impossible for them to credibly demonstrate independence. In the current Chinese political environment, it is inconceivable to think that Chinese companies could meaningfully resist a Chinese government request for access to data or assistance in performing "intelligence work" on any subject related to "national security."[65] The party-state operates with a broad conception of national security and in recent years has been tightening its grip on companies and citizens alike.[66] The CCP has expanded its presence in Chinese corporations, waged a global campaign of cybertheft of foreign IP and data, and launched sweeping domestic digital-surveillance programs.[67] Against this backdrop, there is a considerable risk that, as a 2012 House of Representatives intelligence report concluded regarding Huawei and ZTE, Chinese tech companies "would be obligated to cooperate with any

[64] Andrew Polk, *China is Quietly Setting Global Standards*, Bloomberg (May 6, 2018), https://www.bloomberg.com/opinion/articles/2018-05-06/china-is-quietly-setting-global-standards.
[65] *See* Donald C. Clarke, *The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law* (Mar. 17, 2019), available at https://ssrn.com/abstract=3354211.
[66] *See* Williams, *supra* note 46, at 3-8. *See also, e.g.*, Tom Mitchell & Xinning Liu, *Chinese Communist party asserts greater control over private enterprise*, Fin. Times (Sept. 28, 2020), https://www.ft.com/content/582411f6-fc3b-4e4d-9916-c30a29ad010e.
[67] Robert D. Williams, *Is Huawei a Pawn in the Trade War? The Politics of the Global Tech Race*, Foreign Aff. (Jan. 30, 2019), https://www.foreignaffairs.com/articles/china/2019-01-30/huawei-pawn-trade-war.

request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security."[68]

To be sure, the perception of party-state control over Chinese companies has been overstated in U.S. political discourse. As Meg Rithmire has explained, "Many observers have taken the CCP's renewed role in the economy to mean that any action of a Chinese firm is part of a calculated plan designed by Beijing. This is not the case; rather, much of China's resurgent 'state capitalism' is a reaction to perceived threats, both domestic and foreign. Moreover, the CCP's domestic and international economic goals are pursued through experimental, adaptive, and flexible 'campaign-style' policies rather than premeditated plans with central coordination."[69] Acknowledging the complex tensions at play between the interests of Chinese firms and the Chinese party-state, it is nonetheless difficult to imagine an "Apple vs. FBI" type of standoff with a Chinese technology company refusing to comply with a Chinese government request for access to data in a national security-related investigation.[70] Notwithstanding the implementation of important legal reforms and measures to promote judicial professionalization in recent years, China still lacks an independent judiciary and genuine rule of law. This is particularly true insofar as it relates to "sensitive cases" that might fit within the party-state's sweeping and amorphous definition of national security.[71] Thus, there remain serious constraints

[68] *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger, Permanent Select Committee on Intelligence, U.S. House of Rep. (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[69] Meg Rithmire, *The Resurgent Role of the State in China's Economy: Experimentation, Domestic Politics, and U.S. Policy*, Penn Project on the Future of U.S.-China Relations (Oct. 2020), https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Meg-Rithmire_The-Resurgent-Role-of-the-State-in-China%E2%80%99s-Economy_Final.pdf.

[70] Regarding the Apple/FBI saga, see Leander Kahney, *The FBI Wanted a Back Door to the iPhone. Tim Cook Said No*, Wired (Apr. 16, 2019), https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/. Careful observers of China's data governance system have pointed to discrete instances of companies resisting government requests for data outside the national security context, but still conclude that "there is no guarantee that the government cannot access data because China's system lacks clarity of law, oversight mechanisms and clear pathways for contestation." Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, Lawfare (Apr. 2, 2020), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement.

[71] Fu Hualing, *Duality and China's Struggle for Legal Autonomy*, 1 China Perspectives 3 (2019), https://www.cefc.com.hk/article/editorial-duality-and-chinas-struggle-for-legal-autonomy/. As the Office of the U.S. Trade

on the capacity of market players in China to challenge governmental prerogatives.[72] Again, this is not to suggest that Chinese "digital authoritarianism" is omnipotent, despite some misleading American commentary to that effect.[73] As Samm Sacks has explained, it is a mistake to imagine that the Chinese government has unfettered real-time access to all Chinese companies' data. At the same time, however, U.S. officials must consider the risks inherent in China's governance system with the acknowledgment that "[i]f the Chinese government wants something, they can get it."[74]

iv. Human Rights and Values

These broad political realities of the Chinese system also feed a fourth category of concern: potential threats to human rights and liberal values. There are at least three versions of this challenge. The most direct version considers human rights violations within China and the extent to which Chinese technology companies may be enabling or contributing to those abuses. The most egregious example of such abuse is the high-tech "smart city" apparatus China has implemented to conduct mass surveillance and arbitrary detention of Uyghurs and other ethnic and religious minorities in Xinjiang—even, reportedly, to support population-control measures that amount to genocide.[75] Moreover, reports suggest this surveillance apparatus—including phone scanners, facial-recognition cameras, and biometric databases—is not limited to

---

Representative put it in its April 2020 Special 301 Report, "A truly independent judiciary is critical to promote rule of law in China and to protect IP rights." *2020 Special 301 Report*, Office of the U.S. Trade Rep. (Apr. 2020), at 41 https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf.

[72] *See, e.g.*, Mark Kazmierczak et al., *China's Biotechnology Development: The Role of U.S. and Other Foreign Engagemen*t, Report for the U.S.-China Economic and Security Review Commission (Feb. 14, 2019), at 131-32 ("Furthermore, private companies may voluntarily allow government access to data with the hopes of receiving beneficial treatment in the future, whether through favorable policies, regulatory decisions, or investments.")

[73] *See* Louise Matsakis, *How the West Got China's Social Credit System Wrong*, Wired (July 29, 2019), https://www.wired.com/story/china-social-credit-score-system/.

[74] Sacks, *supra* note 70.

[75] *See* Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Hum. Rts. Watch (May 1, 2019), https://www.hrw.org/report/2019/05/02/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass; Chris Buckley & Paul Mozur, *How China Uses High-Tech Surveillance to Subdue Minorities*, N.Y. Times (May 22, 2019), https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html; *China cuts Uighur births with IUDs, abortion, sterilization*, Assoc. Press (June 29, 2020), https://apnews.com/269b3de1af34e17c1941a514f78d764c; Robert D. Williams, *International law with Chinese characteristics: Beijing and the "rules-based" global order*, Brookings Inst. (Oct. 2020), at 7, https://www.brookings.edu/research/international-law-with-chinese-characteristics-beijing-and-the-rules-based-global-order/.

repression in Xinjiang, but is increasingly widespread and sophisticated throughout mainland China.[76] The relative lack of constraints on the government's ability to access and utilize citizens' data may give China advantages in developing these mass-surveillance systems.[77]

Second, there is an ongoing debate over the degree to which China is exporting its domestic model of digital control along with its exports of cutting-edge surveillance equipment.[78] To the extent Chinese technology companies are actively supporting repression abroad as well as at home, U.S. policymakers may be confronted with questions of whether it is consistent with U.S. values to allow those companies to operate freely in the United States. One need not envision the future of U.S.-China relations as an epic ideological competition between liberal democracy and digital authoritarianism in order to appreciate the stakes of this moral dilemma.[79] Indeed, this is a subset of broader questions concerning the degree to which the future international order will reflect Chinese government values and preferences. Nor is the debate entirely theoretical: human rights advocates argue that China's efforts to influence global technical standards for facial recognition and other technologies at the International Telecommunication Union have "cross[ed] the line from technical specifications to policy recommendations, including outlining use cases and data requirements for facial recognition and

[76] Paul Mozur & Aaron Krolik, *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*, N.Y. Times (Dec. 17, 2019), https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.
[77] *See* Matt Sheehan, *Much Ado about Data: How America and China Stack up*, Macro Polo (July 16, 2019), https://macropolo.org/ai-data-us-china/; Julian Baird Gewirtz, *China's Long March to Technological Supremacy*, Foreign Aff. (Aug. 27, 2019), https://www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy ("Because the CCP already engages in large-scale surveillance and limits personal freedoms, innovations in big-data systems for smart cities and social credit point in a startlingly dystopian direction.").
[78] *See* Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*, Brookings Inst. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf; Laura Rosenberger, *Making Cyberspace Safe for Democracy*, Foreign Aff. (June 2020), https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy; Justin Sherman, *U.S. Diplomacy is a Necessary Part of Countering China's Digital Authoritarianism*, Lawfare (Mar. 17, 2020), https://www.lawfareblog.com/us-diplomacy-necessary-part-countering-chinas-digital-authoritarianism; Steven Feldstein, *When it comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge*, War on the Rocks (Feb. 12, 2020), https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/.
[79] *See* Nicholas Wright, *How Artificial Intelligence Will Reshape the Global Order*, Foreign Aff. (July 10, 2018), https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

other surveillance technologies."[80] Beijing is currently poised to release "China Standards 2035," a fifteen-year strategy to influence global technical standards across a range of cutting-edge industries including telecom and AI.[81] Some see warning signs that China's new Digital Silk Road and infrastructure investment projects may be vehicles for aiding recipient governments in using technology to repress their populations.[82]

Third and finally, policymakers must consider the potential effects of China's domestic surveillance and censorship policies for U.S. domestic politics and the integrity of American democracy. This challenge should not necessarily be confused with that of responding to "sharp power"[83] or "influence operations"[84] that seek to exploit the open information environment of the United States and other liberal democracies to undermine democratic institutions and processes. Regardless of intentionality, there is a risk that certain Chinese domestic policies—particularly those aimed at curating online speech—might be exported to the United States as a negative externality of Chinese tech companies expanding into foreign markets. If Chinese social media apps apply content censorship tools in the United States that they are required by governmental directive to employ domestically in China, this could pose a risk to U.S. values of free speech

[80] Anna Gross et al., *Chinese tech groups shaping UN facial recognition standards*, Fin. Times (Dec. 1, 2019), https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.
[81] *China Standards 2035*, Horizon Advisory, https://www.horizonadvisory.org/china-standards-2035-first-report; Arjun Kharpal, *Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech*, CNBC (Apr. 27, 2020), https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html; Brigitte Dekker et al., *Unpacking China's Digital Silk Road*, Clingendael Inst. (July 2020), at 14-16 ("Yet if Chinese companies in particular play a more prominent role in standard-setting proposals, there is a growing risk of state interests prevailing over a human-centric approach.").
[82] *See* Richard Fontaine & Daniel Kliman, *On China's New Silk Road, Democracy Pays A Toll*, Foreign Pol'y (May 16, 2018), https://foreignpolicy.com/2018/05/16/on-chinas-new-silk-road-democracy-pays-a-toll/; Clayton Cheney, *China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism*, Council on Foreign Rel. (Sept. 26, 2019), https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political; Valentin Weber, *The Worldwide Web of Chinese and Russian Information Controls*, Open Tech. Fund (Sept. 17, 2019), https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf.
[83] Juan Pablo Cardenal et al., *Sharp Power: Rising Authoritarian Influence*, Nat'l Endowment for Democracy (Dec. 2017), https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf.
[84] Rush Doshi & Robert D. Williams, *Is China interfering in American politics?*, Brookings Inst. (Oct. 2, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/. According to the Department of Justice, "Foreign influence operations include covert actions by foreign governments intended to sow divisions in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives." DOJ Justice Manual, *available at* https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730.

and open discourse.[85] On the other hand, potential restrictions on those apps may present their own risks to freedom of expression. Although there is much more to say on this topic,[86] for present purposes the point is simply that it represents a distinct category of values-based concern that shades into a national security challenge in the wake of Russian interference in the 2016 presidential election.[87]

Chinese Companies and Strategic Distrust

The sources of distrust outlined above derive from a blend of national security, economic, political, legal, and moral considerations. In order to understand their practical implications, consider the ways in which these concerns apply to two Chinese companies operating in the strategically significant technological fields discussed previously: 5G and AI.

i. Huawei and 5G[88]

Huawei is the world's largest producer of the equipment needed to operate 5G networks. It is positioned to expand its market share given the low cost of its products,[89] its investment in research and development,[90] and its ability to offer efficient end-to-end solutions that cover devices, networks, and data centers.[91] But the U.S. government and others have raised significant national security concerns about Huawei because of the cybersecurity risks inherent to 5G,

[85] *See, e.g.*, Paul Mozur, *Zoom Blocks Activist in U.S. After China Objects to Tiananmen Vigil*, N.Y. Times (June 11, 2020), https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-square.html; Alex Hern, *Revealed: How TikTok censors videos that do not please Beijing*, Guardian (Sept. 25, 2019), https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.
[86] An additional issue, for example, is the prospect that surveillance of overseas accounts and content could enable these platforms to bolster China's domestic censorship apparatus. *See* Jeffrey Knockel et al., *We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*, Citizen Lab (May 7, 2020), https://citizenlab.ca/2020/05/we-chat-they-watch/.
[87] *See* Williams, *supra* note 36.
[88] Huawei and ZTE are China's two most prominent telecommunications equipment companies, and both have been at the forefront of U.S.-China tensions in the technology sphere. For purposes of illustration, this discussion will focus on Huawei in particular.
[89] Brian Fung, *How China's Huawei took the lead over U.S. companies in 5G technology*, Wash. Post (April 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/?utm_term=.f6f9ac7c2ba2.
[90] Sijia Jiang, *China's Huawei to raise annual R&D budget to at least $15 billion*, Reuters (July 26, 2018), https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169.
[91] Steve McCaskill, *Huawei: We make it cheaper and simpler to deploy 5G*, Tech Radar (Feb. 22, 2019), https://www.techradar.com/news/huawei-we-make-it-cheaper-and-simpler-to-deploy-5g.

Huawei's past business practices, and the nature of the relationship between Chinese tech companies and the Chinese government.

The administration of U.S. President Donald Trump has taken unprecedented actions targeting Huawei. In May 2019, Trump issued an executive order (extended in May 2020[92]) laying the groundwork for a ban on Huawei equipment in U.S. networks. The move expanded restrictions enacted in 2018 regarding the use of Huawei by U.S. agencies and federal contractors.[93] In November 2019, the Federal Communications Commission (FCC) prohibited use of the Universal Service Fund to purchase equipment or services from any company that presents a national security threat to communications networks or the supply chain.[94] In June 2020, the FCC formally designated Huawei and its affiliates (along with ZTE) as posing such a threat.[95] These actions accompanied the enactment in March 2020 of the Secure and Trusted Communications Networks Act, which bans the use of federal telecom subsidy funds to procure equipment or services designated by the FCC as posing an "unacceptable national security risk," and directs the FCC to establish a reimbursement program for small, predominantly rural telecommunications companies to replace any such components in their networks.[96]

In May 2019, the U.S. Department of Commerce (DOC) added Huawei and sixty-eight affiliate firms to the list of entities subject to export restrictions due to the risks they pose to U.S.

[92] Text of a Letter from the President to the Speaker of the House of Representatives and the President of the Senate, White House (May 13, 2020), https://www.whitehouse.gov/briefings-statements/text-letter-president-speaker-house-representatives-president-senate-77.
[93] Executive Order on Securing the Information and Communications Technology and Services Supply Chain, White House (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.
[94] Report and Order, Further Notice of Proposed Rulemaking, and Order, Fed. Trade Comm'n (Nov. 26, 2019), https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.
[95] *FCC Designates Huawei and ZTE as National Security Threats*, Fed. Trade Comm'n (June 30, 2020), https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf.
[96] Secure and Trusted Communications Networks Act of 2019, Public Law 116–124, 116th Cong. (Mar. 12, 2020), https://www.govinfo.gov/content/pkg/PLAW-116publ124/pdf/PLAW-116publ124.pdf.

national security and foreign policy interests.[97] Following these actions, Huawei (and its in-house chip producer HiSilicon) reduced its reliance on U.S. semiconductor manufacturers but continued to source chips from foreign foundries that use American equipment and technology. In May 2020, the Trump administration closed the foreign product loophole by barring companies anywhere in the world—including HiSilicon suppliers Semiconductor Manufacturing International Corporation (SMIC) and Taiwan Semiconductor Manufacturing Company (TSMC)—from using American-made machinery and software to design or produce chips for Huawei or its entities.[98] Then, in August 2020, the Commerce Department expanded the scope of this rule to cover any chips made abroad with American equipment and to any transaction where such products are supplied with knowledge that they will be incorporated into a product directly or indirectly supplied to Huawei. At the same time, DOC placed 38 additional Huawei companies on the Entity List and terminated the temporary license that had previously exempted certain transactions with Huawei relating to cybersecurity and product development.[99] Around the same time, regulations took effect that prohibit the U.S. federal government from buying goods or services from any company that uses products from five Chinese companies, including Huawei.[100]

As of this writing, a growing number of countries have either formally banned or otherwise taken steps to exclude Huawei from their 5G networks. These include Australia, Japan,

[97] Addition of Entities to the Entity List, U.S. Dep't of Commerce (May 21, 2019), https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.
[98] *Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies*, U.S. Dep't of Commerce (May 15, 2020), https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts; Ana Swanson, *U.S. Delivers Another Blow to Huawei with New Tech Restrictions*, N.Y. Times (May 15, 2020), https://www.nytimes.com/2020/05/15/business/economy/commerce-department-huawei.html.
[99] Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List, U.S. Dep't of Commerce (Aug. 17, 2020), https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and; David McCabe & Raymond Zhong, *Trump Administration Widens Huawei Dragnet*, N.Y. Times (Aug. 17, 2020), https://www.nytimes.com/2020/08/17/technology/trump-huawei-commerce-chips.html.
[100] David Shepardson & Mike Stone, *U.S. federal contract ban takes effect for companies using products from Huawei, others*, Reuters (Aug. 13, 2020), https://www.reuters.com/article/us-usa-china-contracting/u-s-federal-contract-ban-takes-effect-for-companies-using-products-from-huawei-others-idUSKCN25928Y.

the United States, the United Kingdom, France, Sweden, India, Vietnam, and Taiwan.[101] Several European countries and Canada had not reached final decisions. The Trump administration has waged a vigorous diplomatic campaign to persuade other countries to reject Huawei.[102] In May and August 2020, the State Department rolled out a multi-country "Clean Network" initiative, one pillar of which is the effort to ensure a "clean path" for 5G communications transiting U.S. diplomatic facilities overseas, which in practice means an "end-to-end communication path that does not use any transmission, control, computing, or storage equipment from untrusted IT vendors, such as Huawei and ZTE."[103]

What's behind this barrage of actions? Some of the U.S. concerns with Huawei are specific to the company itself, but many are structural—both to 5G and to China's governance model. The most fundamental anxiety relates to Huawei's inability to credibly claim independence from the Chinese party-state.[104] The simplest statement of the problem is that, if requested, Huawei would have no choice but to assist the Chinese government in carrying out espionage or sabotage by leveraging its equipment in foreign networks. The potential for such attacks emanating from China, combined with the "critical" nature of 5G infrastructure as outlined above, renders Huawei an unacceptable security risk in the eyes of U.S. officials.

At a technical level, there is evidence that some of Huawei's engineering practices are shoddy and could be exploited by any malicious cyber actor. The United Kingdom's Huawei Cyber Security Evaluation Center, a watchdog that audits the security of Huawei equipment,

---

[101] *See* Joe Panettieri, *Huawei: Banned and Permitted in Which Countries? List and FAQ*, Channel E2E (updated Oct. 23, 2020), https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/.
[102] Justin Sherman, *Is the U.S. Winning Its Campaign Against Huawei?*, Lawfare (Aug. 12, 2020), https://www.lawfareblog.com/us-winning-its-campaign-against-huawei; Michael R. Pompeo, *The Tide Is Turning Toward Trusted 5G Vendors*, U.S. Dep't of State (June 24, 2020), https://www.state.gov/the-tide-is-turning-toward-trusted-5g-vendors/.
[103] The Clean Network, U.S. Dep't of State, https://www.state.gov/the-clean-network/.
[104] It bears noting that Huawei's chief financial officer Meng Wanzhou, who in December 2018 was arrested in Canada for extradition to the United States on fraud charges, reportedly held a passport typically issued only to employees of China's government or state-owned enterprises. When China detained two Canadians in response to Meng's arrest, its ambassador to Canada invoked national "self-defense." *China's ambassador accuses Canada of 'white supremacy' in Huawei CFO arrest*, Guardian (Jan. 9, 2019), https://www.theguardian.com/world/2019/jan/09/china-ambassador-canada-white-supremacy-huawei.

identified in March 2019 a litany of persistent and "concerning issues in Huawei's approach to software development bringing significantly increased risk to UK operators."[105] In fairness, however, few if any of Huawei's corporate competitors have been subjected to the same level of technical scrutiny.

More troubling is the mounting evidence that Huawei has routinely violated local laws in countries where it operates. In January 2019, the U.S. Justice Department accused the company of fraud, money laundering, violating U.S. sanctions against Iran, and stealing trade secrets from its business partner T-Mobile. In February 2020, DOJ charged Huawei and two of its subsidiaries with federal racketeering and conspiracy to steal trade secrets from six American companies.[106] The same month, U.S. national security advisor Robert O'Brien and other U.S. officials stated publicly that they have evidence Huawei maintains covert access to sensitive information in systems it constructs around the world.[107] These reports and other incidents, combined with Huawei's secrecy and mysterious ownership structure,[108] have stoked fears about the company's operations and intentions.

Huawei's risk profile is further complicated by the fact that the company is deeply implicated in structural Chinese economic and trade policies that disadvantage competitors. American and European officials argue that Chinese telecom subsidies give companies like Huawei unfair commercial advantages and leverage in the development and deployment of global networks. According to a *Wall Street Journal* investigation, "Huawei had access to as much as $75 billion in state support as it grew from a little-known vendor of phone switches to

[105] *Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019*, U.K. Cabinet Office (Mar. 28, 2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.
[106] *Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets*, U.S. Dep't of Justice (Feb. 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.
[107] Bojan Pancevski, *U.S. Officials Say Huawei Can Covertly Access Telecom Networks*, Wall St. J. (Feb. 12, 2020), https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.
[108] Tim Rühlig, *Who Controls Huawei? Implications for Europe*, Swedish Inst. Int'l Aff. (May 2020), https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf.

the world's largest telecom-equipment company—helping Huawei offer generous financing terms and undercut rivals' prices by some 30 [percent]."[109] In addition, foreign telecom vendors have complained about a lack of reciprocity in access to the Chinese market through regulatory hurdles that effectively insulated Huawei from competition in the domestic market at the same time that the company expanded its footprint abroad.[110] If Huawei has full access to the European, North American, and Chinese markets while foreign telecoms are prevented from enjoying reciprocal access to the Chinese market, it stands to reason that Huawei could dominate the global 5G market and squeeze out foreign competitors. This outcome would be further assured if, as noted above, Beijing has created an expectation that Huawei and other Chinese companies participating in 3GPP will vote for Chinese-proposed standards regardless of whether they are superior—an additional means of bolstering Chinese companies' hold on the global market.

Finally, Huawei is also a target of concerns around the protection of human rights. Although operational details remain scarce, there is evidence that Huawei is directly enabling the above-mentioned abuses in Xinjiang. Analysts at the Australian Strategic Policy Institute report that "Huawei's work in Xinjiang is extensive and the company works directly with the Chinese Government's public security bureaus, and police forces, in the region."[111] Huawei has provided technical support for "smart policing," including through a data center for Aksu Prefecture and an agreement with the Xinjiang Public Security Bureau to establish an "intelligent security industry" innovation lab in Urumqi.[112] New questions are emerging over the extent to which

[109] Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, Wall St. J. (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.
[110] Morris Lore, *China's Rigged Telecom Market Keeps Nordic Firms in Huawei's Shadow* (Oct. 22, 2019), https://www.lightreading.com/asia-pacific/chinas-rigged-telecom-market-keeps-nordic-firms-in-huaweis-shadow/a/d-id/755034.
[111] *Mapping China's Tech Giants*, Int'l Cyber Policy Center, https://chinatechmap.aspi.org.au/#/company/huawei.
[112] *See id. See also* Nathan Vanderklippe, *Huawei's Partnership with China on Surveillance Technology Raises Concerns for Foreign Users*, Globe & Mail (May 14, 2018), https://www.theglobeandmail.com/world/article-huaweis-partnership-with-china-on-surveillance-raises-concerns-for/.

these technologies and the practices that they enable are being exported. For example, in its 2018 annual report, Huawei claimed that its "safe city solutions now serve over 700 cities across more than 100 countries and regions, including Brazil, Mexico, Serbia, Singapore, Spain, South Africa, and Turkey."[113]

ii. ByteDance/TikTok and AI

Whereas Huawei is China's principal national champion at the cutting edge of 5G equipment, the universe of successful Chinese AI companies is wider and even more dynamic. These include ByteDance, SenseTime, Megvii, Hikvision, iFlytek, Yitu, and a host of others. To illustrate the challenge to U.S. policymakers, this discussion will focus in particular on ByteDance and its social media subsidiary, TikTok.

Founded in 2011 by computer scientist Zhang Yiming, ByteDance is the world's largest technology "unicorn," recently valued at nearly $100 billion.[114] The company's core product, Toutiao, has evolved from a news recommendation engine into a multimedia content delivery platform. Toutiao offers its users personalized information feeds that are powered by algorithms which update content based on machine learning of user preferences. In 2017, ByteDance acquired U.S. video-sharing platform Musical.ly and combined it with Douyin into a single application known as TikTok, a globally popular social-media app boasting more than two billion downloads as of May 2020.[115]

ByteDance is now the only technology company other than Apple with more than 100 million users both in China and in the West.[116] The company continues to expand in the AI arena, recently adding to its portfolio Lingxi, a Beijing-based startup that applies AI to financial

[113] Greitens, *supra* note 78.
[114] *ByteDance is going from strength to strength*, Economist (Apr. 18, 2020), https://www.economist.com/business/2020/04/18/bytedance-is-going-from-strength-to-strength.
[115] Manish Singh, *TikTok tops 2 billion downloads*, Tech Crunch (Apr. 29, 2020), https://techcrunch.com/2020/04/29/tiktok-tops-2-billion-downloads/.
[116] *See ByteDance is going from strength to strength*, *supra* note 114.

services such as debt collection and insurance sales.[117] Leveraging the massive datasets generated by its ever-expanding user base, ByteDance's applications use computer vision, natural language processing, and other forms of AI to understand and analyze written content, images, and videos.[118]

In November 2019, news broke that the interagency Committee on Foreign Investment in the United States (CFIUS) had opened a national security investigation into ByteDance.[119] These reports followed direct appeals to the Committee from members of Congress who urged CFIUS to investigate TikTok's acquisition of Musical.ly. Senator Marco Rubio alleged "ample and growing evidence" that TikTok removes content that is out of step with "Chinese Government and Communist Party directives," such as information related to protests in Hong Kong.[120] In a separate letter to Acting Director of National Intelligence Joseph Maguire, Senators Chuck Schumer and Tom Cotton cited potential national security risks posed by TikTok's collection of users' personal data and the app's content censorship practices.[121]

On August 6, 2020, relying on statutory emergency powers, President Trump issued an executive order prohibiting certain transactions with ByteDance (along with a companion order targeting the messaging app WeChat, owned by Chinese firm Tencent[122]). The TikTok order

[117] Rita Liao, *TikTok parent ByteDance leads $6m round in financial AI startup Lingxi*, Tech Crunch (May 19, 2020), https://techcrunch.com/2020/05/19/bytedance-invests-in-debt-collection-ai-company-lingxi/.
[118] Bernard Marr, *ByteDance Uses Machine Learning to Revolutionize the News*, Forbes (Dec. 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#57c7e2540db8.
[119] Richard Altieri & Benjamin Della Rocca, *U.S. Launches National Security Probe into Chinese-Owned App TikTok*, Lawfare (Nov. 8, 2019), https://www.lawfareblog.com/us-launches-national-security-probe-chinese-owned-app-tiktok.
[120] Letter from U.S. Senator Marco Rubio to U.S. Treasury Secretary Mnuchin (Oct. 9, 2019), https://www.rubio.senate.gov/public/_cache/files/9ba023e4-2f4b-404a-a8c0-e87ea784f440/FCEFFE1F54F3899795B4E5F1F1804630.20191009-letter-to-secretary-mnuchin-re-tiktok.pdf.
[121] Cotton, Schumer Request Assessment Of National Security Risks Posed By China-Owned Video-Sharing Platform, TikTok, A Potential Counterintelligence Threat With Over 110 Million Downloads In U.S., Alone (Oct. 24, 2019), https://www.cotton.senate.gov/?p=press_release&id=1239.
[122] Executive Order on Addressing the Threat Posed by WeChat, White House (Aug. 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/. The WeChat executive order alleges that: "Like TikTok, WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information. . . . WeChat, like

asserted that TikTok's collection of data on U.S. users "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."[123] Eight days later, Trump issued an order based on the CFIUS review that directed ByteDance to divest itself from TikTok within 90 days.[124] In a follow-up announcement on September 17, the Commerce Department accused TikTok of collecting "vast swaths of data from users, including network activity, location data, and browsing and search histories." DOC further alleged that TikTok is "an active participant in China's civil-military fusion and is subject to mandatory cooperation with the intelligence services of the CCP."[125]

Following President Trump's orders, TikTok reached a tentative agreement to partner with Oracle and Walmart to operate its U.S. business.[126] On September 19, Trump announced that he had approved in principle a deal to create a new U.S.-based company, TikTok Global, in which Oracle and Walmart would own 20 percent and Oracle would provide data storage and security services in the United States.[127] (Because ByteDance is 40 percent owned by U.S. investors, the proposed new company could be said to have majority American ownership.[128]) At the time of writing, that deal was pending CFIUS review and approval in addition to review by

---

TikTok, also reportedly censors content that the Chinese Communist Party deems politically sensitive and may also be used for disinformation campaigns that benefit the Chinese Communist Party."

[123] Executive Order on Addressing the Threat Posed by TikTok, White House (Aug. 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ [hereinafter, "TikTok Order"].

[124] Order Regarding the Acquisition of Musical.ly by ByteDance Ltd, White House (Aug. 14, 2020), https://www.whitehouse.gov/presidential-actions/order-regarding-acquisition-musical-ly-bytedance-ltd/.

[125] Wilbur Ross, *Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States*, U.S. Dep't of Commerce (Sept. 17, 2020), https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.

[126] Georgia Wells & Aaron Tilley, *Oracle Wins Bid for TikTok in U.S., Beating Microsoft*, Wall St. J. (Sept. 14, 2020), https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-tiktoks-u-s-operations-11600039821.

[127] Ana Swanson et al., *Trump Approves Deal Between Oracle and TikTok*, N.Y. Times (Sept. 19, 2020), https://www.nytimes.com/2020/09/19/technology/trump-oracle-and-tiktok.html.

[128] Andrew Restuccia et al., *Trump Signs Off on TikTok Deal With Oracle, Walmart*, Wall St. J. (Sept. 19, 2020), https://www.wsj.com/articles/trump-signs-off-on-deal-allowing-tiktok-to-continue-u-s-operations-11600551352.

regulators in Beijing pursuant to new Chinese export restrictions that could prohibit transfer of TikTok algorithms and source code.[129] In the meantime, TikTok is challenging the Trump administration's actions in U.S. courts. On September 27, a federal judge issued a preliminary injunction that temporarily halted the ban on downloading TikTok from U.S. app stores and set the stage for protracted litigation.[130]

The U.S. accusations against TikTok over its data practices exemplify the "data security as national security" quandary identified above. Although Trump's August 6 executive order targeting ByteDance was highly unorthodox, CFIUS has balked before at the prospect of Chinese companies gaining access to U.S. citizen data. In January 2018, the Committee blocked Chinese firm Ant Financial's bid to acquire U.S. payments company MoneyGram over data access concerns analogous to those cited by the Trump administration in its warnings about TikTok.[131] Months later, CFIUS ordered Beijing Kunlun Tech, a Chinese gaming company, to sell dating app Grindr over fears that the Chinese government might gain access to data that could be used to blackmail users of the app.[132]

As outlined above, concerns about Beijing's access to U.S. citizen data are altogether legitimate. On the other hand, experts have called into question the intelligence value of the data

---

[129] Paul Mozur et al., *TikTok Deal Is Complicated by New Rules From China Over Tech Exports*, N.Y. Times (Aug. 29, 2020), https://www.nytimes.com/2020/08/29/technology/china-tiktok-export-controls.html; Zhou Xin & Tracy Qu, *TikTok's algorithm not for sale, ByteDance tells US: source*, S. China Morning Post (Sept. 13, 2020), https://www.scmp.com/economy/china-economy/article/3101362/tiktoks-algorithm-not-sale-bytedance-tells-us-source.

[130] *See* Robert Chesney, *TikTok Wins Round One: An Overview of Judge Nichols's Preliminary Injunction Ruling*, Lawfare (Sept. 28, 2020), https://www.lawfareblog.com/tiktok-wins-round-one-overview-judge-nicholss-preliminary-injunction-ruling (explaining that the injunction "concerns *only* the International Emergency Economic Powers Act (IEEPA) sanctions, *not* the separate [CFIUS] order compelling ByteDance to divest itself of TikTok by mid-November"); Abby Lemert & Eleanor Runde, *U.S. Courts Halt Bans on Chinese Apps*, Lawfare (Oct. 7, 2020), https://www.lawfareblog.com/us-courts-halt-bans-chinese-apps (summarizing the preliminary injunction related to TikTok and describing a similar stay issued by a federal court against the WeChat order).

[131] Greg Roumeliotis, *U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns*, Reuters (Jan. 2, 2018), https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7.

[132] Echo Wang, *China's Kunlun Tech agrees to U.S. demand to sell Grindr gay dating app*, Reuters (May 13, 2019), https://www.reuters.com/article/us-grindr-m-a-beijingkunlun/chinas-kunlun-tech-agrees-to-u-s-demand-to-sell-grindr-gay-dating-app-idUSKCN1SJ28N.

that TikTok collects.[133] Some note that its personal information collection practices are similar to those of many other non-Chinese apps.[134] These observations raise the question of whether a generalized concern about Chinese government access to data constitutes a sufficient national security justification for excluding a Chinese company from the U.S. market. As for the Commerce Department's accusation that TikTok is an "active participant" in China's civil-military fusion program, at the time of writing DOC had not provided details on the nature of that relationship or its assessment of the security implications.

Further complicating this picture, the U.S. government has pointed not only to the security implications of U.S. citizen data collection, but also to TikTok's alleged content censorship and disinformation practices. According to the August 6 executive order, "TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities. This mobile application may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus."[135]

The language about TikTok's reported censorship may refer to media reports such as a September 2019 article in *The Guardian*, according to which ByteDance's content moderation guidelines showed that TikTok moderators had at one point been instructed to "censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong."[136] In addition, *The New York Times* cited an anonymous former content moderator for

[133] James A. Lewis, *How Scary is TikTok?*, CSIS (July 14, 2020), https://www.csis.org/analysis/how-scary-tiktok; Samm Sacks, *Banning TikTok is a Terrible Idea*, SupChina (July 16, 2020), https://supchina.com/2020/07/16/banning-tiktok-is-a-terrible-idea/.
[134] Louise Matsakis, *Does TikTok Really Pose a Risk to US National Security?*, Wired (July 17, 2020), https://www.wired.com/story/tiktok-ban-us-national-security-risk/.
[135] TikTok Order, *supra* note 123.
[136] Alex Hern, *Revealed: how TikTok censors videos that do not please Beijing*, Guardian (Sept. 25, 2019), https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

TikTok who claimed that "managers in the United States had instructed moderators to hide videos that included any political messages or themes, not just those related to China," thus preventing them from being shared more widely than individual users' feeds.[137] (This practice is known as "shadow banning.")

Assuming such reports are accurate, there is at least arguably a national security dimension to the censorship allegation that does not conflate national security imperatives with free speech values. Evidence that an ostensibly private company is manipulating content to serve the ends of the Chinese party-state could help to reveal whether and how the company is subject to direction from that state. The extent of TikTok's censorship is hotly contested, but the basic concern is valid: if an app is censoring for Beijing, it might also be handing over data to Beijing.

The censorship-as-national-security claim also operates at a higher level of abstraction. Following Russia's interference in the 2016 U.S. presidential election, American officials are sensitized to the risk of foreign interference in the U.S. information environment, which is foundational to the functioning of American democracy.[138] Few Americans are eager to import Chinese state media narratives and curated information flows. But at what point does government propaganda or lobbying activity become a sovereignty-violating "information operation"? When does influence cross the line into interference? And should open societies that value the "marketplace of ideas" respond to these perceived threats with governmental bans on channels of communication? Doing so directly implicates the right to free expression under the First Amendment of the U.S. Constitution.[139]

---

[137] Jack Nicas et al., *TikTok Said to Be Under National Security Review*, N.Y. Times (Aug. 7, 2020), https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.
[138] *See* Doshi & Williams, *supra* note 84.
[139] These questions also apply to U.S. restrictions on Tencent's WeChat app. The Commerce Department issued an order banning downloads of the WeChat app from U.S. app stores by midnight on September 20, 2020. The rules would prohibit software updates to the app, although they do not specifically prohibit "exchange between or among WeChat mobile application users of personal or business information using the WeChat mobile application, to include the transferring and receiving of funds." *Identification of Prohibited Transactions to Implement Executive Order 13943 and Address the Threat Posed by WeChat and the*

These complexities are compounded by the dual-use potentiality of AI and the economic and security advantages that can accrue to companies and governments that have access to global datasets. Could ByteDance's position enable it to squeeze foreign competitors out of important markets for developing data-driven technologies? What might the company do with its dominant market position? Will it be a benign market actor or a vector for censorship and surveillance? To what extent will the Chinese government seek to access and exploit ByteDance's data in ways inimical to U.S. national security and liberal values?

A different version of the values question—one not specified in President Trump's executive order—focuses on ByteDance's possible role in enabling human rights abuses domestically within China. Much discussion about Chinese AI companies' involvement in government repression in Xinjiang and other parts of China has focused on companies directly engaged in developing the facial recognition software and surveillance equipment that is used for programs such as the Integrated Joint Operation Platform (IJOP) for predictive policing. In October 2019, eight such entities—Dahua Technology, iFlytek, Megvii Technology, SenseTime, Xiamen Meiya Pico Information Co. Ltd., Yitu Technologies, and Hikvision—were added to the U.S. Entity List and subjected to export restrictions for activities deemed contrary to U.S. foreign policy interests. The Commerce Department described these companies as being "implicated in human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uighurs, Kazakhs, and other members of Muslim minority groups in [Xinjiang]."[140] Nine additional Chinese tech companies

---

National Emergency with Respect to the Information and Communications Technology and Services Supply Chain, 15 CFR Ch. VII [Docket No. 200917-0248], U.S. Dep't of Commerce (Sept. 17, 2020), https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-20921.pdf. The morning of September 20, a federal judge in California issued a preliminary injunction temporarily blocking the restrictions on WeChat, citing First Amendment concerns. Sebastian Herrera & Katy Stech Ferek, *WeChat Ban Is Blocked By Federal Judge In Ruling Against Trump Administration*, Wall St. J. (Sept. 20, 2020), https://www.wsj.com/articles/wechat-ban-is-blocked-by-federal-judge-in-ruling-against-trump-administration-11600609504.

[140] Addition of Certain Entities to the Entity List, U.S. Dep't of Commerce (Oct. 9, 2019), https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-22210.pdf.

were added to the Entity List in May 2020, followed two months later by the addition of another 11 companies.[141]

Less attention has been paid to subtler forms of technological support to repressive policies, such as propaganda support. Although ByteDance does not produce surveillance hardware and has not been subjected to U.S. export controls, a recent report by the Australian Strategic Policy Institute alleges that ByteDance "collaborates with public security bureaus across China, including in Xinjiang where it plays an active role in disseminating the party-state's propaganda on Xinjiang."[142] This cooperation reportedly goes beyond the Xinjiang authorities' use of ByteDance platforms to disseminate propaganda. It includes a strategic cooperation agreement that ByteDance signed with the Ministry of Public Security in April 2019 to promote the "influence and credibility" of police departments across China.[143] Details of such cooperation remain scarce and further research is required to determine the extent and nature of ByteDance's activities that might enable human rights abuses (beyond the "ordinary" censorship practices required to operate in Mainland China). But policymakers cannot ignore these multi-layered questions raised by Chinese AI companies, including ByteDance.

Conclusion and Recommendations

The preceding discussion is intended to highlight—not to resolve—the complex range of issues raised by the actual and potential effects of Chinese technology companies operating in

[141] *Commerce Department to Add Nine Chinese Entities Related to Human Rights Abuses in the Xinjiang Uighur Autonomous Region to the Entity List*, U.S. Dep't of Commerce (May 22, 2020), https://www.commerce.gov/news/press-releases/2020/05/commerce-department-add-nine-chinese-entities-related-human-rights; *Commerce Department Adds Eleven Chinese Entities Implicated in Human Rights Abuses in Xinjiang to the Entity List*, U.S. Dep't of Commerce (July 20, 2020), https://www.commerce.gov/news/press-releases/2020/07/commerce-department-adds-eleven-chinese-entities-implicated-human.

[142] Fergus Ryan et al., *Mapping* More *of China's Technology Giants: AI and Surveillance*, ASPI Int'l Cyber Pol'y Ctr. (Nov. 2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-12/Mapping%20more%20of%20Chinas%20tech%20giants.pdf?wpDVHlKgXJHzeK8rZ.kmy0Ei63RxXMO.

[143] Shi Yang, *China's Ministry of Public Security's Propaganda Office Announces Strategic Collaboration with ByteDance* [公安部新闻宣传局与字节跳动战略合作签约暨全国公安新媒体矩阵入驻今日头条抖音仪式举行] (Apr. 25, 2019), https://web.archive.org/web/20191127235720/http://news.cpd.com.cn/n3559/201904/t20190425_836599.html.

the United States. To summarize, this complexity is a function of several phenomena. The increasing importance and dual-use nature of cutting-edge technologies such as 5G and AI heightens potential risks to national security and feeds a policy mindset that equates data security with national security. With Chinese tech companies expanding overseas, those technological risks must be evaluated through the lens of China's political-legal system. Relevant features of that system include Beijing's expressed strategic ambitions, its economic policies and practices to advance those ambitions, the relative lack of effective rule-of-law constraints to check the party-state's exercise of power over tech companies, and the related challenge of assessing the ways in which new technologies may threaten human rights and liberal values in China and in overseas markets for Chinese technology.

Although Huawei and TikTok-owner ByteDance illustrate the confluence of these thorny strategic and moral challenges, in some ways the two companies are atypical cases. Cybersecurity is a widespread problem, to be sure, but Huawei is distinctive in that its 5G business directly implicates the building of critical telecom infrastructure.[144] Similarly, even though the controversy over TikTok reveals the range of factors relevant to data protection, no other Chinese internet platform currently has a comparable footprint in the U.S. market. Indeed, TikTok is arguably "the first Chinese company to truly break through to the American, and global, consciousness."[145]

Still, it is clear that Huawei and ByteDance demonstrate the omni-use problem, the blurring of data privacy and national security, and the impetus for defensive U.S. policy responses based on "worst-case" assumptions about China's governing system. Many of these considerations merge traditional conceptions of national security, economic interests, and values-

[144] Jamie Smyth, *Australia banned Huawei over risks to key infrastructure*, Fin. Times (Mar. 27, 2019), https://www.ft.com/content/543621ce-504f-11e9-b401-8d9ef1626294.
[145] Michael Schuman, *Why America Is Afraid of TikTok*, Atlantic (July 30, 2020), https://www.theatlantic.com/international/archive/2020/07/tiktok-ban-china-america/614725/.

based policy objectives that defy simple categorization in terms of discrete risks to "national security."

Clarifying the relevant technological risks does not by itself resolve the question of how to evaluate those factors against the potential downsides of measures to reduce risk exposure.[146] There are innumerable costs and benefits associated with U.S.-China technological and economic interdependence, and policies that reduce integration in the name of security could also negate points of leverage that would otherwise redound to national security in the long run. Yet U.S. policy cannot be calibrated by relying on abstract notions of "interdependence" or "decoupling." Nor is the challenge readily amenable to universal decision rules to balance risk and opportunity in all cases. But complexity does not absolve U.S. policymakers of the burden to develop a more sustainable policy framework.

In recent years, Washington has often appeared reactive and incoherent in its approach to cybersecurity and technology policy, focusing excessively on a few Chinese companies while largely shirking the responsibility to develop a positive governance vision. 5G cyber risks are much broader than Huawei,[147] and similarly, the need for stronger data protection applies not just to TikTok but to all companies that process information on U.S. citizens, regardless of where they are incorporated.[148] The United States cannot, and should not, seek to out-compete China at its own game: banning companies, censoring apps, and barring the free flow of information and ideas. There remains an opportunity to chart a more productive and affirmative course. To that end, the following policy initiatives should be prioritized.

---

[146] *See* Stu Woo, *The U.S. vs. China: The High Cost of the Technology Cold War*, Wall St. J. (Oct. 22, 2020), https://www.wsj.com/articles/the-u-s-vs-china-the-high-cost-of-the-technology-cold-war-11603397438.
[147] *See* Wheeler & Williams, *supra* note 12; Williams, *supra* note 9.
[148] *See* Sacks, *supra* note 70.

Enact Federal Data Privacy Legislation

The executive branch should work with Congress to enact legislation establishing a federal data privacy framework with clear standards for the collection, processing, and sharing of personal data.[149] The California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR) have already begun to catalyze such privacy legislation.[150] The goal should be to improve upon these market-shaping laws to set "highest common denominator" standards for data brokers operating in the U.S. market, regardless of national origin, while sustaining broadly free flows of data across national borders. The law should be enforceable through a combination of federal regulatory powers and private rights of action.

The challenge of striking the proper balance should not be underestimated. Data openness and security are two sides of the same coin: sometimes security calls for access and openness, other times for protection and mitigation. But with a coherent data protection regime in place that addresses principles—not nationalities—there would be less need to resort to exceptional presidential authorities for one-off bans or divestment orders regarding specific Chinese technology companies. The United States for years has complained about the fact that American tech platforms such as Google, Facebook, YouTube, Twitter, and WhatsApp are prohibited in China.[151] The appropriate response to China's arbitrary application of "national security" is not to imitate the Chinese approach.[152] Where principles-based privacy and consumer protection laws fail to address specific risks, CFIUS can provide an effective, narrowly tailored mechanism

[149] *See, e.g.*, Jennifer Daskal & Samm Sacks, *The Furor Over TikTok Is About Something Much Bigger*, Slate (Nov. 8, 2019), https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html.
[150] *See generally* Anupam Chander et al., *Catalyzing Privacy Law*, Minn. L. Rev. (forthcoming 2020), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433922.
[151] *See* Ana Swanson et al., *Trump Administration to Ban TikTok and WeChat From U.S. App Stores*, N.Y. Times (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html.
[152] For example, among the downsides of the recent U.S. restrictions on WeChat is the fact that they may impair the ability of U.S. multinational companies to use the app for certain business purposes in China. Given that WeChat has become an indispensable platform "at the center of digital life in China," the new U.S. policy could turn out to be a gift to America's competitors in the Chinese market. *Id.*

to safeguard national security while restoring confidence in the United States' open economic system.[153]

Work with Allies and Partners on Digital Trade

In tandem with domestic legislative reform, the United States should seek to find common ground on digital trade with countries that have strong commitments to data security and interoperability, inspired by Japan's proposal for "data free flow with trust."[154] Over the past four years, Washington has lost ground in setting the terms of debate on cross-border data flows. An enforceable digital trade agreement among a club of like-minded nations could benefit American workers and the innovation base while creating long-term incentives for countries such as China to improve their domestic governance regimes and cut back on state-sponsored theft of foreign IP.

Digital trade negotiations will be complicated, especially with European counterparts, but the effort may not be as politically difficult as it sounds. For example, the provisions on digital trade in the 11-country Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) largely cohere with those in the U.S.-Mexico-Canada Agreement (USMCA)[155] and the U.S.-Japan Digital Trade Agreement (USJDTA).[156] Indeed, USMCA and USDJTA rules are even more comprehensive than those in the CPTPP.[157] There is thus precedent that can be

[153] In related contexts, I have argued that the United States' overly broad invocation of "national security" to justify recent trade-related actions against China risks undermining its own longstanding positions against Chinese practices, a dynamic that can be described as a "reciprocity of hypocrisy." *See* Robert D. Williams, *The Commerce Department's Self-Defeating Conception of National Security*, Lawfare (Feb. 26, 2018), https://www.lawfareblog.com/commerce-departments-self-defeating-conception-national-security.

[154] *See* Nigel Cory et al., *Principles and Policies for "Data Free Flow With Trust"*, Info. Tech. & Innovation Found. (May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

[155] United States-Mexico-Canada Agreement, July 1, 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

[156] Agreement Between the United States of America and Japan Concerning Digital Trade, Jan. 1, 2020, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf.

[157] *See* Comparison of Selected Digital Trade Provisions in the United States-Mexico-Canada Agreement (USMCA) and the Trans-Pacific Partnership (TPP), BSA (Apr. 11, 2019), https://www.bsa.org/files/policy-filings/04112019tppvusmcacomparison.pdf

expanded and strengthened to promote security and interoperability across borders. This will require, among other things, that U.S. and EU officials identify broadly shared interests when it comes to data governance—an agenda that recently has been overshadowed by controversies over the U.S.-EU Privacy Shield.[158]

Establish a Cybersecurity Liability Regime

The American tort regime has not caught up to the challenge of properly incentivizing companies to invest in cyber hygiene. The compromise of personal data on U.S. citizens held by Equifax, Marriott, Anthem, and others did not require Chinese ownership of those companies. The negative externalities of poor cybersecurity practices can impose a mix of harms to consumers, industries, and national security. The U.S. Cyberspace Solarium Commission (CSC) has proposed that Congress pass a law "establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities."[159] Software vendors should be responsible for developing and distributing patches in a timely manner, and companies should be encouraged to disclose vulnerabilities and implement the basic steps needed to ensure they are regularly updating their systems. These duties of care could be accompanied by requirements for IoT producers to certify the security of systems built into their products and to clarify cyber risks for consumers over the life cycle of their products.

Cybersecurity liability reform would complement national data privacy legislation. Despite some overlap, the former aims to protect sensitive data held by private companies from malicious cyber intrusions; the latter sets the terms on which companies may lawfully collect and

[158] *See* Catherine Stupp, *Officials Warn Privacy Shield Replacement May Be a Long Way Off*, Wall St. J. (Sept. 8, 2020), https://www.wsj.com/articles/officials-warn-privacy-shield-replacement-may-be-a-long-way-off-11599557400; Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security*, VoxEU (Aug. 5, 2020), https://voxeu.org/article/impact-gdpr-data-flows-and-national-security.
[159] *Report of the United States Cyberspace Solarium Commission* (Mar. 2020), at 76, https://www.solarium.gov/report.

utilize consumer data. To help facilitate a data security liability framework, the federal government could convene private sector and academic experts to improve the modeling and pricing of cyber risks in creating a functional market for cybersecurity insurance.[160]

Increase the Costs for Malicious Hackers

At the same time that the United States seeks to incentivize companies to invest in cybersecurity, it should also pursue creative means to deter and disrupt malicious cyber actors. Chinese state-linked hackers have not been appreciably deterred by the recent spate of DOJ indictments for cybertheft on U.S. networks where there is no realistic chance of extraditing or prosecuting the defendants.[161] Recent reports suggest the U.S. government may be expanding its "defend forward" strategy aimed at disrupting malicious cyber activities at their source, including activities below the threshold of armed conflict.[162] Although clear signaling is needed to ensure such actions do not spark escalation, the U.S. should expand these efforts to impose meaningful costs for specific, attributable incidents of cybertheft.[163]

As a next step, Washington should endeavor to organize a coalition of like-minded states to enforce norms against commercial cybertheft. This could be done through discrete, targeted multilateral sanctions against entities that engage in and benefit from operations for which attribution can be accomplished publicly and jointly with partner governments.[164] Multilateral sanctions have already been deployed against Russian hackers and, under existing U.S.

---

[160] *See id.* at 81.
[161] *See* Goldsmith & Williams, *supra* note 49; Williams, *supra* note 31.
[162] Erica D. Borghard & Mark Montgomery, *Defend Forward as a Whole-of-Nation Effort*, Lawfare (Mar. 11, 2020), https://www.lawfareblog.com/defend-forward-whole-nation-effort; Rosen Remarks, *supra* note 53 ("[T]he Department of Justice and the FBI have been working with seven private sector partners, including Microsoft Corporation, Google, Facebook, and Verizon Media, to identify and neutralize the computer infrastructure that APT-41 uses to conduct its crimes: its virtual private servers, malware, malicious domains, and other tools. We have done this through a combination of public and private actions, including technical measures to block this threat actor from accessing victims' computer systems, issuing a public safety announcement outlining their tactics, techniques, and procedures (to aid network defenders), and by taking control of, or otherwise disabling, their accounts pursuant to court orders or terms of service violations.").
[163] *See* Ben Buchanan & Robert D. Williams, *A Deepening U.S.-China Cybersecurity Dilemma*, Lawfare (Oct. 24, 2018), https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma.
[164] *See* Lorand Laskai, *A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage*, Council on Foreign Rel. (Dec. 6, 2018), https://www.cfr.org/report/threat-chinese-espionage.

authorities, could be incorporated into a broader package of sticks and carrots to address Chinese state-sponsored cyber activity.

Improve Domestic and International Policy Coordination

Cybersecurity and technology policy issues cut across the domains of economics, national security, and political values. Coherent policy thus requires a multi-disciplinary approach informed by sound technical expertise. Bearing this in mind, the next U.S. administration should consider establishing an interagency, CFIUS-like coordinating group to examine the practical implications of prospective technology policies such as export controls, entity listings, supply chain risk standards, immigration policies, subsidies, and more. Whether designed as a joint committee with a lead agency (perhaps housed in the Commerce Department) or as an expansion and elevation of the White House Office of Science and Technology Policy (with enhanced oversight power), the group would seek to ensure that federal policies are as narrowly tailored as possible to protect sensitive technologies without cutting off the lifeblood of their development: data, investment, and human capital.[165]

Such an entity should have the flexibility to coordinate innovation policy proposals among allies and partners. For example, in consultation with allied governments, the U.S. could devise a plan to provide intra-group economic opportunities for countries with varying threat perceptions to join together in adopting tailored export controls and other protections.[166] As suggested by the authors of a recent report arguing for an "alliance innovation base," a suite of incentives could include pooling of data, funding for innovation, and reduction of licensing and

[165] *See* Williams, *supra* note 21.

[166] On export controls, for example, the coordinating group could determine the policy calibration appropriate for restrictions on the sale of semiconductor manufacturing equipment by studying, among other issues, how such policies can be most effectively coordinated with countries such as Japan and the Netherlands that possess advanced photolithography technologies. It could also investigate the tradeoffs in whether to allow U.S. chipmakers to continue selling commodity chips to Huawei while restricting the export of the most advanced semiconductors and chip fabrication equipment. *See* James A. Lewis, *Managing Semiconductor Exports to China*, CSIS (May 5, 2020), https://www.csis.org/analysis/managing-semiconductor-exports-china; Asa Fitch & Kate O'Keeffe, *Qualcomm Lobbies U.S. to Sell Chips for Huawei 5G Phones*, Wall St. J. (Aug. 8, 2020), https://www.wsj.com/articles/qualcomm-lobbies-u-s-to-sell-chips-for-huawei-5g-phones-11596888001.

regulatory barriers to cooperation.[167] The coordinating group could advise on multilateral principles for supply chain security, building on inclusive statements such as the May 2019 Prague Proposals[168] and the EU Toolbox on 5G Security.[169] It could guide joint funding for research and development on Open RAN and other potential software-based solutions to 5G cybersecurity.[170] It could spur the launch of a new multi-stakeholder initiative aimed at ensuring the scientific independence of international standard-setting bodies for 5G and other technologies—monitoring and publicizing efforts by governments and their proxies to manipulate technical standard-setting processes.[171] And it could advise on how to craft sanctions and articulate clear diplomatic signals for entities that enable human rights abuses through the use of digital tools for surveillance and repression, especially in Xinjiang.

In carrying out these functions, the coordinating group would benefit from consulting a range of perspectives, including technical and subject-matter experts outside the federal government. In a domain where hard-and-fast decision rules are elusive, multiple voices are needed to help the U.S. "game out" the downstream consequences of mooted policies and to calibrate strategies that account for the competing values and interests at stake.[172]

---

[167] Daniel Kliman et al., *Forging an Alliance Innovation Base*, Ctr. New Am. Sec. (Mar. 2020), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Alliance-Innovation-Base-Final.pdf?mtime=2020032917490.

[168] *Prague 5G Security Conference announced series of recommendations: The Prague Proposals*, Gov't of the Czech Republic (Mar. 5, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[169] *Secure 5G Networks: Questions and Answers on the EU Toolbox*, Eur. Commission (Jan. 29, 2020), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

[170] Dwight Weingarten, *Open RAN Bill Included in Senate NDAA, Sen. Warner Pushes for More Funding,* MeriTalk (June 30, 2020), https://www.meritalk.com/articles/open-ran-bill-included-in-senate-ndaa-sen-warner-pushes-for-more-funding/.

[171] Jack Kamemsky, *China's Participation in International Standards Setting: Benefits and Concerns for U.S. Industry*, China Bus. Rev. (Feb. 7, 2020), https://www.chinabusinessreview.com/chinas-participation-in-international-standards-setting-benefits-and-concerns-for-us-industry/.

[172] For example, outside experts may be better positioned than government officials to estimate the consequences that could ensue if U.S. companies that rely on the Chinese market begin developing two sets of technological inputs for their products: one developed in China for the Chinese market, and another for everywhere else. This could limit companies' ability to achieve economies of scale and continue to innovate, and at the same time it could facilitate the growth of new competitors in China. On the current trajectory, some companies may find they have little choice but to locate more research and development outside the United States and avoid using U.S. technology that could be blocked at any time—thus undercutting American jobs and competitiveness. Sweeping restrictions on AI "exports" could cause firms to reduce or redirect their AI research and development when confronted with the costs of a cumbersome licensing and compliance process. As David Edelman has warned, doing so "would almost certainly give Chinese companies that don't face those same restrictions a sizable advantage in the playing field."

***

The foregoing proposals constitute just a slice of an agenda for improving the U.S. approach to technological security and innovation. Much of the work in this area will involve investing at home to strengthen American competitiveness while upholding constitutional values. That effort depends far less on China's behavior than it does on America's political choices.

Overall, these proposals reflect the view that U.S. policymakers should widen the aperture of their approach. Concerns about cybersecurity and data protection are not limited to China and cannot be addressed only through country- or company-specific measures. Over the long term, principled policies that are generally applicable and (where possible) multilateral stand the best chance of shaping a future favorable to U.S. interests.

In sum, the United States should aim to set high standards addressing the economic, security, and values-based concerns that many industrialized democracies broadly share when it comes to the risks and opportunities of new technologies. In turn, those standards will raise the bar for Chinese companies that seek to enter the United States and other non-Chinese markets. Perhaps, in this way, China's global technological ambitions will be confronted with competing incentives that push the Chinese regime to moderate those practices that most engender strategic distrust. This outcome is far from preordained—perhaps even a long shot on current trends—but the effort to achieve it should not be abandoned in the service of a self-defeating isolationism that all but guarantees it will not come to pass.

Karen Hao, *A US attempt to keep AI out of China's hands could actually help China*, MIT Tech. Rev. (Nov. 21, 2018), https://www.technologyreview.com/2018/11/21/66366/a-us-attempt-to-keep-ai-out-of-chinas-hands-could-actually-help-china/.