MAY 4, 2023

TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Hearing on Rule by Law: China's Increasingly Global Legal Reach

The Dangers of the Global Spread of China's Digital Authoritarianism

BY

Paul Scharre

Vice President and Director of Studies
Center for a New American Security

I. China's Digital Authoritarianism

Chairman Bartholomew, Vice Chairman Wong, Commissioner Goodwin, Commissioner Helberg, and distinguished Commission members, thank you for the opportunity to testify on the important topic of the Chinese Communist Party's increasingly global legal reach.

China is pioneering a new brand of digital authoritarianism at home and abroad, which poses a profound threat to global freedoms. The United States must work with other democratic nations to push back on these illiberal uses of technology and develop an alternative vision for using digital technologies that preserves personal privacy and individual freedom.

The Chinese Communist Party is using technology to build a dense web of digital and physical surveillance to track and monitor its citizens.[1] Over half of the world's one billion surveillance cameras are in China.[2] Elements of this technology-enhanced authoritarianism in China include:

- Artificial intelligence tools such as facial, voice, and gait recognition;
- Biometric databases consisting of fingerprints, blood samples, voiceprints, iris scans, facial images, and DNA;
- Facial recognition scanners in airports, hotels, banks, train stations, subways, factories, apartment complexes, and public toilets;
- Physical security checkpoints that include searching cell phones for unauthorized content;
- Wi-Fi "sniffers" to gather data from nearby phones and computers;
- License plate readers to identify and track vehicles;
- Police cloud computing centers to churn through data;
- Police software that tracks individuals' movements, car and cell phone use, gas station and electricity use, and package delivery;
- "Minority identification" facial recognition systems that deliberately target minority groups, specifically China's Uighur population; and
- A national "social credit system" consisting of a series of different databases, scores, and blacklists to enhance social and political control over Chinese citizens.[3]

The most extreme version of this techno-authoritarianism exists in Xinjiang, where the Chinese Communist Party is carrying out a brutal campaign of genocide and repression against the ethnic Uighur population. However, many of these tools are used nationwide. COVID-related measures have further enhanced the Chinese Communist Party's control over citizen movements.

Unlike in the United States and other democratic societies, there are no legal constraints on the Chinese Communist Party's ability to surveil its citizens. While China has passed a number of laws and regulations pertaining to cybersecurity, data, and artificial intelligence, the law serves a different purpose in China than in democratic states. Unlike the democratic concept of "rule of law," where the law constrains even the government, China has a system of

[1] Portions of this testimony are drawn from Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence*, (New York: W.W. Norton & Company, 2023).

[2] Liza Lin and Newley Purnell, "A World with a Billion Cameras Watching You Is Just Around the Corner," *Wall Street Journal*, December 6, 2019, https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402.

[3] Kendra Schaefer et al., *Understanding China's Social Credit System* (Trivium China, September 23, 2019), http://socialcredit.triviumchina.com/wp-content/uploads/2019/09/Understanding-Chinas-Social-Credit-System-Trivium-China-20190923.pdf.

"rule by law."[4] The Chinese Communist Party stands above the law, and the law is a vehicle to aid the Party in governing.

Many of China's surveillance systems today are fragmented and imperfect. However, the Party is working to improve them. China's initial efforts to control the internet twenty years ago were similarly imperfect. Yet the Chinese Communist Party has done what many believed impossible and today exercises an incredible degree of control over the information environment inside China through censorship and government propaganda.

China is building the foundation today for an unprecedented system of technology-enhanced repression and control. General Secretary Xi Jinping has said the goal of China's social credit system is to ensure that "Everything is convenient for the trustworthy, and the untrustworthy are unable to move a single step."[5]

II. The Global Spread of China's Model

China's model of digital authoritarianism is spreading abroad, in part due to active promotion by the Chinese Communist Party. At least 80 countries have adopted Chinese police and surveillance technology.[6] Even more troubling is the export of Chinese-style norms and laws for governing cyberspace and digital technologies, the "social software" of this new model of techno-authoritarianism.

Left unchecked, the spread of China's model of technology-enhanced repression poses a profound challenge to global freedoms and individual liberty. The Chinese Communist Party spreads its model of digital authoritarianism through multiple vehicles, including Chinese ownership over critical digital infrastructure, other countries adopting Chinese-style norms and laws, and Chinese involvement in technical standard-setting bodies.

Critical Digital Infrastructure

The global adoption of Chinese surveillance technology facilitates Chinese control over critical digital infrastructure, such as telecommunications networks and social media platforms. Chinese ownership of critical digital infrastructure provides data for Chinese companies to improve their algorithms and opportunities for Chinese government surveillance.

Several countries, including the United States, have banned Huawei equipment because of concerns about spying. In 2018, the French paper *Le Monde* revealed that data was being secretly transferred from the African Union's new headquarters building in Ethiopia, which was financed by the Chinese government and built by Huawei, every night between midnight and 2 a.m. to servers in Shanghai.[7] A subsequent sweep for bugs found hidden microphones under desks and in the walls.[8] Huawei technicians have also reportedly helped the governments of Uganda and Zambia spy

[4] " 'Rule of Law' or 'Rule by Law'? In China, a Preposition Makes All the Difference," *Wall Street Journal*, October 20, 2014, https://www.wsj.com/articles/BL-CJB-24523.

[5] "Component 3: Rewards and Punishments," in Schaefer et al., *Understanding China's Social Credit System*.

[6] Sheena Greitens, " 'Surveillance with Chinese Characteristics': The Development & Global Export of Chinese Policing Technology" (paper presented at Princeton University's International Relations Faculty Colloquium, Princeton, New Jersey, October 7, 2019), 2, http://ncgg.princeton.edu/IR%20Colloquium/GreitensSept2019.pdf.

[7] Danielle Cave, "The African Union Headquarters Hack and Australia's 5G Network," *The Strategist*, July 13, 2018, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/; Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin [In Addis Ababa, the headquarters of the African Union spied on by Beijing]," *Le Monde*, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; Karishma Vaswani, "Huawei: The Story of a Controversial Company," BBC News, March 6, 2019, https://www.bbc.co.uk/news/resources/idt-sh/Huawei; Huawei, "Statement on Huawei's Work With the African Union," 2021, https://www.huawei.com/us/facts/voices-of-huawei/statement-on-huaweis-work-with-the-african-union.

[8] Aaron Maasho, "China Denies Report It Hacked African Union Headquarters," Reuters, January 29, 2018, https://www.reuters.com/article/us-africanunion-summit-china/china-denies-report-it-hacked-african-union-headquarters-idUSKBN1FI2I5.

on political opponents.[9] Huawei is not unique in these concerns. Any Chinese company can be compelled to aid the government in spying abroad.

The Chinese-owned social media platform TikTok presents a threat to U.S. national security because of the risk of U.S. persons' data being exfiltrated to China and TikTok manipulating content on the platform.[10] On numerous occasions, TikTok has appeared to censor political content, including:

- Posts uploaded using #BlackLivesMatter and #GeorgeFloyd;[11]
- A viral video criticizing the Chinese government's treatment of Muslims;[12]
- Clips of "tank man" (the unknown protestor who stood in front of a column of tanks in Tiananmen Square in 1989);[13]
- Videos of Hong Kong pro-democracy protestors;[14] and
- Content relating to the Houston Rockets basketball team, whose general manager had publicly sided with Hong Kong protestors.[15]

In addition to these apparent censorship incidents, independent researchers have found a glut of pro-Chinese Communist Party propaganda videos about Xinjiang on TikTok.[16]

Leaked documents have demonstrated TikTok's systemic manipulation and censorship of political content. In 2019, *The Guardian* newspaper revealed TikTok's leaked moderation guidelines, which included censorship of political content. The bans included prohibiting videos of "highly controversial topics, such as . . . inciting the independence of . . . Tibet and Taiwan," "demonisation or distortion of local or other countries' history such as . . . Tiananmen Square incidents," and "criticism/attack towards policies, social rules of any country, such as . . . socialism system".[17]

The Chinese Communist Party knows the power of controlling information. Just as it has controlled information within China, Chinese ownership over global social media and information platforms allows the Party to extend its reach outside of China, censoring content that it deems offensive or against the Party's interests.

---

[9] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[10] Fergus Ryan, Danielle Cave, and Vicky Xiuzhong Xu, *Mapping More of China's Technology Giants* (report no. 24/2019, Australian Strategic Policy Institute, 2019), https://www.aspi.org.au/report/mapping-more-chinas-tech-giants; Fergus Ryan, Audrey Fritz, and Daria Impiombato, *TikTok and WeChat* (report no. 37/2020, Australian Strategic Policy Institute, 2020), https://www.aspi.org.au/report/tiktok-wechat.

[11] Vanessa Pappas and Kudzi Chikumbu, "A Message to Our Black Community," Tiktok news release, June 1, 2020, https://newsroom.tiktok.com/en-us/a-message-to-our-black-community.

[12] Brenda Goh, "TikTok Apologizes for Temporary Removal of Video on Muslims in China," Reuters, November 27, 2019, https://www.reuters.com/article/us-bytedance-tiktok-xinjiang/tiktok-apologizes-for-temporary-removal-of-video-on-muslims-in-china-idUSKBN1Y209E.

[13] Yaqiu Wang, "Targeting TikTok's Privacy Alone Misses a Larger Issue: Chinese State Control," Human Rights Watch, January 24, 2020, https://www.hrw.org/news/2020/01/24/targeting-tiktoks-privacy-alone-misses-larger-issue-chinese-state-control.

[14] Drew Harwell and Tony Romm, "TikTok's Beijing Roots Fuel Censorship Suspicion as It Builds a Huge U.S. Audience," *Washington Post*, September 15, 2019, https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/.

[15] Ben Thompson, "The China Cultural Clash," *Stratechery* (blog), October 8, 2019, https://stratechery.com/2019/the-china-cultural-clash/.

[16] Ryan, Fritz, and Impiombato, *TikTok and WeChat*, 15–17.

[17] Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *The Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

Chinese ownership over a major U.S. social media platform poses unacceptable risks to U.S. national security. Congress should pass legislation giving the Executive Branch the authority to address threats from foreign ownership in critical information and telecommunications technologies.

Norms and Laws

China has been active in promoting its norms for governing cyberspace and surveillance technologies. According to Freedom House, China has held training sessions and seminars with over thirty countries on cyberspace and information policy.[18] Examples include a two-week "Seminar on Cyberspace Management" held in 2017 for officials from countries participating in China's Belt and Road Initiative. In 2018, journalists and media officials from the Philippines visited China to learn about "socialist journalism with Chinese characteristics." Similar Chinese media conferences have brought in representatives from Egypt, Jordan, Lebanon, Libya, Morocco, Saudi Arabia, Thailand, and the United Arab Emirates. At the government-run Baise Executive Leadership Academy in southern China, over 400 government officials from southeast Asian countries have been trained in "China's governance and economic development model," including how to "guide public opinion" online.[19]

Other countries have begun adopting Chinese-style laws for digital technologies. In Tanzania, Uganda, and Vietnam, restrictive media and cybersecurity laws closely followed Chinese engagement.[20] Zimbabwe's government, whose officials have attended Chinese seminars, has been enthusiastic about following China's lead.[21] In 2018, Zimbabwe signed a strategic partnership with the Chinese company CloudWalk to build a mass facial recognition system consisting of a national database and intelligent surveillance systems at airports, railways, and bus stations.[22] Former Zimbabwean ambassador to China Christopher Mutsvangwa said the deal would help "spearhead our AI revolution in Zimbabwe."[23] In 2021, Zimbabwe's government adopted a new cybersecurity law modeled on China that has been criticized for undermining human rights.[24] Many authoritarian states are all too eager to learn from China's model of surveillance, censorship, and repression.

Technical Standards

China has also begun playing a more active role in international technical standard-setting bodies, using them as another vehicle for exporting China's vision of digital illiberalism. Technical standards are an important avenue for shaping global development of technology. International standards organizations include the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the UN International Telecommunication Union (ITU). Since 2018, the Chinese government has been increasingly active in international standard-setting bodies, along with major Chinese tech firms such as Huawei, ZTE, Tencent, SenseTime,

---

[18] Adrian Shahbaz, *Freedom on the Net 2018* (Freedom House, 2019), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[19] He Huifeng, "In a Remote Corner of China, Beijing Is Trying to Export Its Model by Training Foreign Officials the Chinese Way," *South China Morning Post*, July 14, 2018, https://www.scmp.com/news/china/economy/article/2155203/remote-corner-china-beijing-trying-export-its-model-training.

[20] Shahbaz, *Freedom on the Net 2018*.

[21] David Gilbert, "Zimbabwe Is Trying to Build a China Style Surveillance State," *Vice*, December 1, 2019, https://www.vice.com/en_us/article/59n753/zimbabwe-is-trying-to-build-a-china-style-surveillance-state.

[22] Shan Jie, "China Exports Facial ID Technology to Zimbabwe," *Global Times*, April 12, 2018, http://www.globaltimes.cn/content/1097747.shtml.

[23] Problem Masau, "Zimbabwe: Chinese Tech Revolution Comes to Zimbabwe," *Herald* (Zimbabwe), October 9, 2019, https://allafrica.com/stories/201910090185.html.

[24] Council of the EU, "Zimbabwe: Declaration by the High Representative on behalf of the European Union," press release, February 21, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/02/21/zimbabwe-declaration-by-the-high-representative-on-behalf-of-the-european-union/; MISA Zimbabwe, "Analysis of the Data Protection Act," December 6, 2021, https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/.

iFLYTEK, Dahua, and China Telecom.[25] The Chinese government released a "White Paper on Artificial Intelligence Standardization" in 2018 and a national strategy for technical standards in 2021.[26]

Technical standards can affect how technology enables or undermines personal privacy and individual freedoms. In 2019, leaked documents from the United Nations ITU standards process, which covers 193 member states, showed delegates considering adopting rules for facial recognition tech that would help facilitate Chinese-style norms of surveillance.[27] For example, requirements in the draft rules included storing a person's race in a database, enabling the kind of technology-enhanced racial profiling that China has adopted. China's influence in technical standards-setting bodies threatens to spread standards that would enable Chinese-style surveillance and repression worldwide.

III. A Democratic Alternative

The spread of China's model of digital repression intersects with a troubling global rise in authoritarianism. Since the mid-2000s, the world has been experiencing a "wave of autocratization," with authoritarian leaders tightening their grip and democracies experiencing "democratic backsliding," such as reduced checks on executive authority.[28] "Digital dictators" are on the rise, leveraging social media, censorship, and surveillance to enhance control over their population.[29] The United States and other democratic nations must work together to push back against these trends and present an alternative model for using digital technologies in a way that preserves personal privacy and individual freedom.

---

[25] Jeffrey Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *DigiChina* (blog), NewAmerica.org, June 20, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/; Justus Baron and Olia Kanevskaia Whitaker, "Global Competition for Leadership Positions in Standards Development Organizations," SSRN, March 31, 2021), https://ssrn.com/abstract=3818143; Marta Cantero Gamito, "From Private Regulation to Power Politics: The Rise of China in AI Private Governance Through Standardisation," SSRN, February 28, 2021, https://ssrn.com/abstract=3794761; U.S.-China Economic and Security Review Commission, *2021 Report to Congress,* November 2021, https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf; U.S.-China Economic and Security Review Commission, Chapter 1, Section 2, "The China Model: Return of the Middle Kingdom," in 2020 Annual Report to Congress, December 2020, 80–135, https://www.uscc.gov/sites/default/files/2020-12/Chapter_1_Section_2--The_China_Model-Return_of_the_Middle_Kingdom.pdf; "Will China Set Global Tech Standards?," ChinaFile, March 22, 2022, https://www.chinafile.com/conversation/will-china-set-global-tech-standards; "Chinese Involvement in International Technical Standards: A DigiChina Forum," DigiChina, December 6, 2021, https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/; Daniel R. Russel and Blake H. Berger, *Stacking the Deck: China's Influence in International Technology Standards Setting* (Asia Society Policy Institute, November 2021), https://asiasociety.org/sites/default/files/2021-11/ASPI_StacktheDeckreport_final.pdf; Bradley A. Thayer and Lianchao Han, "We Cannot Let China Set the Standards for 21st Century Technologies," *The Hill*, April 16, 2021, https://thehill.com/opinion/technology/548048-we-cannot-let-china-set-the-standards-for-21st-century-technologies/; Alexandra Bruer and Doug Brake, "Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy," Information Technology & Innovation Foundation, November 8, 2021, https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy; Jacob Feldgoise and Matt Sheehan, "How U.S. Businesses View China's Growing Influence in Tech Standards," Carnegie Endowment for International Peace, December 23, 2021, https://carnegieendowment.org/2021/12/23/how-u.s.-businesses-view-china-s-growing-influence-in-tech-standards-pub-86084.

[26] "中共中央国务院印发《国家标准化发展纲要》[The Central Committee of the Communist Party of China and the State Council issued the "National Standardization Development Outline"], Central Committee of the Communist Party of China—State Council, October 10, 2021, http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm; English translation here: "Translation: The Chinese Communist Party Central Committee and the State Council Publish the 'National Standardization Development Outline'," Center for Strategic and Emerging Technology, November 19, 2021, https://cset.georgetown.edu/publication/the-chinese-communist-party-central-committee-and-the-state-council-publish-the-national-standardization-development-outline/; Matt Sheehan, Marjory Blumenthal, and Michael R. Nelson, *Three Takeaways From China's New Standards Strategy* (Carnegie Endowment for International Peace, October 28, 2021), https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678.

[27] Anna Gross, Madhumita Murgia, and Yuan Yang, "Chinese Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[28] Anna Lührmann and Staffan I. Lindberg, "A Third Wave of Autocratization Is Here: What Is New About It?" *Democratization* 26, no. 7 (2019), https://doi.org/10.1080/13510347.2019.1582029; Nancy Bermeo, "On Democratic Backsliding," *Journal of Democracy* 27, no. 1 (January 2016): 5–19, https://www.journalofdemocracy.org/articles/on-democratic-backsliding/.

[29] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs*, March/April 2020, https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.

Our work begins at home. The United States government has taken a largely laissez-faire approach to digital governance, deferring regulating tech companies. This has enabled the growth of "surveillance capitalism" in which U.S. companies hoover up massive amounts of personal data. The U.S. Congress has considered, but has not passed, a comprehensive federal data privacy law. The United States has a patchwork of laws at the state and sometimes local level governing digital technologies, including consumer data privacy and law enforcement use of facial recognition. Without regulation, corporate policies vary widely. Social media companies, for example, have varying approaches to regulating disinformation and AI-generated synthetic media, such as deepfakes.

One of the challenges in developing a democratic alternative to digital governance is that the U.S. process for developing new laws involves a messy give-and-take among a diverse array of stakeholders: federal, state, and local governments, businesses, academia, the media, civil society, and grassroots movements of concerned citizens. Input from diverse stakeholders will lead to a better outcome in the long run, leading to rules that balance the interests of different elements of society. But is a slower process. The Chinese Communist Party can simply dictate by fiat how China will govern new digital technologies. In democratic societies, the process of establishing rules for governing new technologies can be slower but will lead to better outcomes overall. It is vitally important that the United States accelerate this process of developing rules governing digital technologies, both to ensure that these technologies are used for beneficial purposes in American society and to help shape emerging global norms.

IV. Recommendations

Key steps the U.S. government can take to address the growing dangers of the spread of China's model of digital authoritarianism include:

- **The United States must accelerate legislation governing digital technologies.** Congressional leadership is needed to create nationwide rules governing digital technologies. Congress should pass a comprehensive federal data privacy law. Additionally, Congress should pass legislation governing AI-generated synthetic media, requiring disclosure to users when content such as text, voice, images, or video is generated by artificial intelligence. Congress should also work with social media companies to establish common standards for combating disinformation, manipulative content, and inauthentic behavior, informed by industry best practices.

- **The U.S. Congress must take steps to protect critical U.S. digital infrastructure from Chinese ownership.** The U.S. government has been active in addressing the risks from Huawei in 5G telecommunications networks. However, TikTok's Chinese ownership remains a continued concern. Chinese ownership of a major U.S. social media platform is an unacceptable threat to U.S. national security. Congress should pass legislation giving the Executive Branch the authority to address threats from foreign ownership in critical information and telecommunications technologies.

- **The U.S. government should become more engaged in shaping emerging global norms for digital governance.** Technical standards are an important vehicle for shaping how technology is used globally, and the U.S. government should become more engaged in supporting technical standard-setting bodies to ensure the integrity of the standard-setting process.[30] Congress should increase funding for the National Institute of Standards and Technology (NIST) to ensure it is adequately funded to engage in international standard-setting discussions.

[30] James Olthoff, "Setting the Standards: Strengthening U.S. Leadership in Technical Standards," NIST, March 17, 2022, https://www.nist.gov/speech-testimony/setting-standards-strengthening-us-leadership-technical-standards.

- **The United States must work with democratic allies to present a shared vision for governing cyberspace and artificial intelligence.** The U.S. State Department and Commerce Department should work with allies to lead the establishment of a new grouping of technology-leading democratic states. Sometimes referred to as a "Tech 10," "T-12," or "T-14," such a grouping would consist of the G7 nations (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) plus other technology-leading democracies, such as Australia, the European Union, Finland, India, Israel, the Netherlands, South Korea, and Sweden.[31] The United States has already taken steps to increase collaboration with allies in Europe and the Indo-Pacific region through the U.S.-EU Trade and Technology Council (TTC) and the Quad. The United States should double-down on these efforts while expanding cooperation to include additional like-minded countries to shape global norms and standards for digital technologies.

Appendix

This testimony reflects the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

[31] Anja Manuel, "How to Win the Technology Race with China," Freeman Spogli Institute for International Studies, June 18, 2019, https://fsi.stanford.edu/news/how-win-technology-race-china; Anja Manuel, Pavneet Singh, and Thompson Paine, "Compete, Contest and Collaborate: How to Win the Technology Race with China," Stanford Cyber Policy Center, October 17, 2019, https://fsi.stanford.edu/publication/compete-contest-and-collaborate-how-win-technology-race-china; Martijn Rasser et al., *Common Code: An Alliance Framework for Democratic Technology Policy* (Center for a New American Security, October 21, 2020), https://www.cnas.org/publications/reports/common-code; Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies: How to Build Digital Cooperation," *Foreign Affairs*, November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; David Howell, "It's Time to Replace the Outmoded G7," *Japan Times*, February 15, 2021, https://www.japantimes.co.jp/opinion/2021/02/15/commentary/world-commentary/g7-g20-d10-uk-russia-us-boris-johnson/; Marietje Schaake, "How Democracies Can Claim Back Power in the Digital World," *MIT Technology Review*, September 29, 2020, https://www.technologyreview.com/2020/09/29/1009088/democracies-power-digital-social-media-governance-tech-companies-opinion/; Joe Biden, "My Trip to Europe Is About America Rallying the World's Democracies," *Washington Post*, June 5, 2021, https://www.washingtonpost.com/opinions/2021/06/05/joe-biden-europe-trip-agenda/.