Statement before the

Congressional-Executive Commission on China

"Techno-Authoritarianism: Platform for Repression in China and Abroad."

A Testimony by:

Jonathan E. Hillman

Senior Fellow, Economics Program, and

Director, Reconnecting Asia Project, CSIS

Wednesday, November 17, 2021

106 Dirksen Senate Office Building

Chairman Merkley, Chairman McGovern, and distinguished Members of the Commission, thank you for holding this important hearing and asking me to participate.

This testimony draws from my book, *The Digital Silk Road: China's Quest to Wire the World and Win the Future*, and related research at the Center for Strategic and International Studies, where I direct the Reconnecting Asia Project.[1]

The bottom line is that China is gaining globally through its Digital Silk Road and positioning itself to reap commercial and strategic rewards, but its dominance is far from assured. The United States has several advantages, including world-leading research universities, innovative companies, deep pools of private capital, openness to immigrants, and a global network of partners and allies. The question is whether the United States can rise to the challenge and lead a coalition that offers real benefits to the developing world. In much of the world, cost trumps security. Competing will require expanding the availability of affordable alternatives.

If uncontested, China's Digital Silk Road will undermine U.S. economic and strategic interests. Developing economies will rise in the coming decades, as underscored by demographic trends, and offer vast opportunities for growth.[2] For example, Nigeria, the world's twenty-eighth largest economy in 2017, is projected to become the world's ninth largest economy by 2100. During the same period, India will move from seventh to third place. These projections provide a glimpse of an emerging world that the United States can engage with, and benefit U.S. workers and companies, or allow China to cement a position of strength.

China also stands to gain intelligence and coercive powers if it achieves its global network ambitions. It could have eyes and ears not merely walking around foreign capitals but woven into foreign government buildings, public security command posts, and data centers. It could learn about scientific breakthroughs as they are made, corporate mergers and acquisitions as they are contemplated, and patents before they are filed. On "the worst possible day," Beijing could disrupt, disable, or destroy its adversaries' communications, financial markets, and military systems.[3]

These risks must be taken seriously because the warning signs are already here. For five years, servers at the African Union headquarters sent data to Beijing covertly in the dead of night. Cameras watching over Pakistani streets came equipped with hidden hardware while others malfunctioned. A Chinese subsea cable that stretches from Africa to South America added little but debt to Cameroon's economy. Laos's first satellite is actually majority-owned by Beijing. These are the signs of digital dependency.

---

[1] Jonathan E. Hillman, *The Digital Silk Road: China's Quest to Wire the World and Win the Future* (New York: Harper Business, 2021); Jonathan E. Hillman, *The Emperor's New Road: China and the Project of the Century* (New Haven: Yale University Press, 2020); "Reconnecting Asia Project," Center for Strategic and International Studies, Accessed November 12, 2020, https://reconasia.csis.org.

[2] Gulrez Azhar, et al. "Fertility, morality, migration, and population scenarios for 195 countries and territories from 2017 to 2100: a forecasting analysis for the Global Burden of Disease Study." *The Lancet*, 396, no. 10258 (2020). Doi: https://doi.org/10.1016/S0140-6736(20)30677-2.

[3] Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *Prism 8*, no. 3, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Donahue_14-35.pdf.

The testimony that follows describes how we got here, provides a tour of the battlefield, and outlines what the United States needs to do. First, it explains how U.S. mistakes paved the way for China's telecommunications giants. Second, it provides an overview of the global digital infrastructure competition in four areas: wireless networks, smart cities, internet backbone, and satellites. Third, it explains why a coalition is necessary to compete, identifies partners, and notes areas of friction that must be managed. Finally, it summarizes recommendations for U.S. policy.

I. Learning from Past Mistakes

The Digital Silk Road sits at the intersection of Chinese leader Xi Jinping's signature policy efforts. It is the technology dimension of China's Belt and Road Initiative, Xi's vision for moving China closer to the center of everything through infrastructure projects, trade deals, people-to-people ties, and policy coordination. By helping Chinese tech companies expand into foreign markets, it also advances "Made in China 2025," which aims to capture dominant market shares in high-tech industries.

The Digital Silk Road was first mentioned in 2015, as the "Information Silk Road," but its roots run much further back. During the 1980s and 1990s, Chinese leaders fashioned industrial policies and negotiated deals with foreign companies that helped Chinese telecommunications firms dramatically improve their capabilities. Through the Digital Silk Road, China aims to further reduce its dependency on foreign companies while making more of the world dependent on Chinese technology.

Conventional narratives usually overlook or oversimplify this longer history. The story often told in Washington is that Huawei and other Chinese firms essentially lied, cheated, and stole their way to success. To be sure, there was plenty of unfair and illegal behavior, from receiving massive state support to blatantly copying competitors' products. But this oversimplified narrative is dangerously self-serving. It avoids taking responsibility, misses mistakes, and offers little insight for competing more effectively. An honest assessment leads to three hard truths:

1. **U.S. leaders overhyped the benefits of connectivity**. Triumphant in the aftermath of the Cold War, U.S. commentators predicted that the Chinese Communist Party (CCP) was digging its own grave by adopting satellite TV, the internet, and other communications systems at home. But CCP leaders set out to modify and wield these tools for their own purposes. Today, commentators warn that China is exporting authoritarianism. In reality, telecommunications systems are tools, neither inherently good nor bad. Understanding impacts, and fashioning solutions, requires looking closely at local contexts.

2. **Foreign companies rushed into China and helped to create their own competitors**. Foreign manufacturers handed over access to their knowledge and capabilities, consultants helped transform Chinese companies' business operations, and researchers went to work for their former companies' competitors. After China's domestic telecommunications capabilities matured, Chinese officials restricted market access for foreign companies. Avoiding these mistakes in emerging technologies will require closer public-private cooperation among the United States, its partners, and allies.

3. **Chinese companies expanded into overlooked markets**. U.S. companies focused primarily on larger, wealthier markets, leaving Chinese providers to serve lower-income and rural markets. Even as Chinese tech companies now face greater scrutiny in advanced economies, they are still building a position of strength in emerging markets, where most of the world's population growth is expected. To compete in those markets, the United States and its partners have to offer affordable alternatives.

II. Navigating the Battlefield

China's Digital Silk Road is advancing in four key areas: wireless networks, smart cities, internet backbone, and satellites. While not exhaustive of China's digital activities, these activities literally stretch from the ocean floor to outer space, and they enable artificial intelligence (AI), big data applications, and other strategic technologies. In all four areas, China is gaining globally and positioning itself to reap commercial and strategic rewards, but its dominance is far from assured. It also has vulnerabilities and weaknesses that the United States and its allies could exploit.

Wireless Networks

The world is beginning to splinter between countries that use Chinese suppliers for their wireless networks and those that do not. The latter category is primarily wealthy democracies. Most NATO member states have raised barriers to Huawei's participation in their 5G rollouts. Australia and Japan have imposed restrictions as well. India has not made a final judgement, but it did not include any Chinese suppliers in its initial 5G trials.

In most of the developing world, however, Chinese providers are moving ahead. They are often the incumbent providers in these markets, having won significant market share after offering equipment at prices 20-30 percent below their competitors. For example, Huawei is believed to have supplied roughly 70 percent of Africa's 4G networks. 5G networks are often built on top of existing networks, and the cost of starting over may appear prohibitive for lower-income countries.

Open Radio Access Networks (Open RAN) could tilt the playing field in favor of the United States. By virtualizing parts of the network that are currently served by proprietary hardware, Open RAN allows operators to mix and match different network components from different vendors. For operators, the potential upside is greater vendor choice, lower deployment costs, and less risk of being locked into a single vendor. The United States stands to benefit because its companies are leading providers of the specialized software and semiconductors that Open RAN relies upon.

Open RAN could take anywhere from several years to a decade to mature. There are already promising examples of Open RAN being deployed around the world, at all speeds, from 2G to 5G. But the flip side of greater vendor choice is greater complexity. There are still kinks to work out as networks combine components from different suppliers. Smaller operators may not have the necessary technical expertise, while larger operators may not have the patience. Some may still prefer the ease of going with a single vendor, even if it is more expensive.

But the 5G race is just getting started. A third of the world's population lives in countries where 1GB mobile broadband plans are unaffordable for average earners. Among those with mobile connections, only 15 percent of users are expected to use 5G by 2025, while nearly 60 percent of mobile users will rely on 4G. The global market is still up for grabs, and the United States can

establish a position of strength by making targeted investments at home and expanding financing and training activities abroad, as outlined below in Part IV.

Smart Cities

Megatrends in innovation and urbanization are turning cities into ground-zero for competing approaches to development and governance.[4] The arrival of faster networks, cheaper sensors, and more sophisticated analytics promises to help reduce crime, ease traffic, and improve other public services, while also impacting civil liberties, data security, and other public concerns. By 2030, seven out of ten people in the world will live in cities, with urban populations growing fastest in Africa and Asia. Around the world, planners will need to decide which systems and safeguards to adopt.

China's "safe city" model, which emphasizes security applications such as surveillance cameras, is gaining traction. Only China has companies that are competitive at every step of the surveillance process, from manufacturing cameras to training AI to deploying the analytics. At home, Chinese companies never question the government's use of these capabilities, and government subsidies fuel their global expansion. Hikvision and Huawei are China's leading providers globally, followed by Dahua and ZTE. Altogether, Chinese firms have exported smart city products and services to more than 100 countries.[5]

These firms offer attractive capabilities at cut-rate prices. Using their "safe city" systems, they claim, will reduce crime, increase economic growth, and even help fight the Covid-19 pandemic. Facial recognition and behavior analysis identifies wanted criminals and alerts the police to unusual behavior, such as wandering near restricted areas. Measuring traffic flows and enforcing driving laws improves congestion. Temperature-sensing cameras identify people with fevers. These and other capabilities can be fed into a central database and command center. Offers that come with financing can give the impression that these systems will essentially pay for themselves.

But China's "safe city" exports are also vulnerable in several respects. Cases in Kenya, Pakistan, and elsewhere show crime rising, cameras malfunctioning, and other challenges.[6] Greater transparency and accountability would surely unearth more instances of overpromising and underdelivering. Chinese firms have also been willing to sell to essentially anyone, creating reputational risks. Over time, companies that press forward without safeguards may find their clientele shrinking to a list of names they would not care to advertise.

These missteps open the door for the United States and its allies to provide alternatives. For example, they could offer a "Sustainable City" certification with financial support that emphasizes commercial viability, energy efficiency, social safeguards, and data security. This is another area

[4] Jonathan E. Hillman and Laura Rivas, "Global Networks 2030," Center for Strategic and International Studies, March 29, 2021, https://www.csis.org/analysis/global-networks-2030-developing-economies-and-emerging-technologies.
[5] Katherine Atha et al., "China's Smart Cities Development," SOS International, January 2020, https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.
[6] Sheridan Prasso, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype," Bloomberg, November 12, 2019, https://www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny.

where U.S. domestic renewal and global competitiveness are strongly aligned. More cutting-edge examples of smart cities at home—such as Charlotte, Las Vegas, and Pittsburgh—will position U.S. companies to succeed abroad.

Internet Backbone

China is redrawing the internet as it builds key connections and nodes, especially subsea cables and data centers, beyond its borders. Its biggest moves are happening in Asia, Africa, and Latin America, where Chinese tech companies face less scrutiny and demand for digital infrastructure is expected to grow significantly in the coming years. Africa, for example, is home to 17 percent of the world's population but less than 1 percent of the world's installed data center capacity. If China's asymmetric strategy for global data flows is successful, its firms will carry, store, and mine more of the world's data while its domestic networks will move further out of foreign reach.

In just a decade, China has graduated from being dependent on foreign companies for subsea cables, which carry over 95 percent of the world's international data, to controlling the world's fourth major provider of these systems. Before being sold to Hengtong Group in 2020, Huawei Marine (a joint venture between Huawei and Global Marine, a UK firm) laid enough cable to circle the earth, including transcontinental links from Asia to Africa and from Africa to South America. These connections avoid U.S. and allied territory and could become even more valuable during a conflict.

China's cloud providers are also marching into emerging markets. The leading U.S. cloud providers—Amazon, Microsoft, and Google—have a massive first-mover advantage. But the Chinese government is following a familiar playbook: pushing data localization rules that favor its providers, leveraging state financing, and packaging services with hard infrastructure. Foreign governments and businesses may find it difficult to switch providers down the road. On top of the normal expenses of migrating from one cloud to another, they may also face Chinese economic coercion.

Meanwhile, the Chinese government is tightening its control over networks at home. Like a medieval castle, China's domestic network forces international connections into a handful of chokepoints and requires foreign carriers to use one of China's "Big Three" state-owned telecom firms (China Telecom, China Mobile, and China Unicom). This architecture gives Beijing an unrivaled ability to monitor, censor, and cut off traffic. Wealthier and more technically savvy individuals can find ways to access the global internet, although popular tools such as virtual private networks (VPNs) have been heavily curtailed.

But China's asymmetric strategy also comes with costs. Restricting access to the global internet harms the ability of Chinese firms to innovate, and restricting international connections leaves even China's Big Three dependent upon foreign carriers for international data transit. Roughly 80 percent of China's international traffic passes through U.S. and European carriers.[7] Mainland Chinese cities are absent among the rankings of the world's most connected hubs, which all have

[7] Dave Allen, "Analysis by Oracle Internet Intelligence Highlights China's Unique approach to Connecting to the Global Internet," Oracle, July 19, 2019, https://web.archive.org/web/20210512021539/https://blogs.oracle.com/internetintelligence/analysis-by-oracle-internet-intelligence-highlights-china%E2%80%99s-unique-approach-to-connecting-to-the-global-internet.

open internet exchanges, a model that remains anathema to Party leaders. The CCP's conundrum is that greater international connectivity requires giving up some control.

The United States and its allies have several enduring advantages in this domain. The United States remains the world's leading hub for internet traffic, a position made possible by its open approach to data flows, innovative companies, and attractive market. The top three subsea cable providers are based in the U.S., Europe, and Japan and are responsible for nearly 90 percent of the global market. Three U.S. companies control over half of the global market for cloud services, and the quality of their offerings is consistently ranked higher than their Chinese competitors. Maintaining these advantages, however, will require competing in tomorrow's markets.

Satellites

China has gone from latecomer to leading provider of satellite services, especially for developing markets. Following major events in the 1990s, particularly the Gulf War and the 1996 Taiwan Strait Crisis, China set out to develop its own global navigation satellite system. Completed in 2020, China's BeiDou system is more accurate than the Global Positioning System (GPS) in the Asia-Pacific region, although slightly less accurate globally, and its satellites occupy fewer orbital planes, making maintenance easier. The system also allows users to send short text messages, and its larger footprint increases its availability. In 165 capital cities, BeiDou provides more extensive coverage than GPS.[8]

BeiDou advances both China's commercial and military interests. When China exports electronics, increasingly it is exporting the BeiDou system, which is included in phones, vehicles, farm equipment, and consumer products. In 2019, China's satellite navigation sector pulled in $64 billion, and by 2029, the global market for satellite navigation devices is projected to grow to about $360 billion. BeiDou includes even more powerful services that guide Chinese missiles, fighter jets, and naval vessels. China has begun offering these military-grade services to partners and could use them as a sweetener in the future when selling arms. Strategically, China is reducing its reliance on GPS and increasing its partners' reliance on BeiDou.

China is also carving out a niche as the go-to provider for developing countries that want their own communications satellites. For about $250 million, only a fraction of which is required up front due to Chinese state financing, countries can acquire their own geostationary communications satellite. China also provides ground stations, testing, training, launch, and operations support. As of early 2021, at least nine countries have bought or are in the process of buying communications satellites from China. Several satellites have experienced launch or operational challenges, and many of China's customers have struggled financially.

Low-earth orbit (LEO), between 500 and 2,000 kilometers high, is the next frontier for competition. LEO broadband constellations could expand access to low-latency, high-speed internet globally. In addition to reaping commercial rewards, nations with leading LEO broadband providers could enjoy increased resiliency in their communications, accuracy in positioning services, and enhanced early warning capabilities. A small group of primarily U.S. and European companies, including SpaceX, Amazon, and OneWeb, are on the cutting edge of these efforts.

[8] Toru Shima, "In 165 Countries, China's Beidou eclipses American GPS," Nikkei Asia, November 25, 2020, https://asia.nikkei.com/Spotlight/Century-of-Data/In-165-countries-China-s-Beidou-eclipses-American-GPS.

Some are using intersatellite-laser links, which allow satellites to exchange data without passing through a ground-based intermediary, increasing performance and complicating government attempts to monitor communications.

China has its own LEO plans. Its companies are behind in the race to launch LEO constellations, but they have generous state support, making profitability less of an immediate concern. This second-mover, state-led strategy allows China to see what works and emulate foreign successes. Some countries may prefer China's alternative, which will surely favor state control of communications. If the LEO competition turns into a marathon, Beijing could also leverage its lending along the Belt and Road to obtain landing rights and obstruct competing efforts.

If the United States seizes this opportunity, the coming wave of LEO constellations could undercut China's advantage in overlooked markets. Western LEO broadband providers could serve rural and less-wealthy markets without building all the ground infrastructure that has deterred them in the past. Some financial assistance—from U.S. and allied governments, multilateral development banks, or even philanthropists—will be required to make these services affordable in low-income markets. Commercial diplomacy, outlined in Part IV, could help U.S. providers secure landing rights.

III. Leading a Coalition

China presents a challenge of scale. Its population of 1.4 billion provides Chinese companies with preferred access to the world's largest market of middle-class consumers and the government with access to an ocean of data. The Chinese government's ability to direct resources, even if inefficient and wasteful, is giving a boost to emerging technologies and subsidizing the cost of Chinese equipment globally.

Meeting this challenge will require the United States to lead a coalition. In the absence of a coalition, China can pit companies against each other to access their technology, just as it did during the 1980s and 1990s, when U.S. and allied telecom companies undercut each other in their race to access China's market. Without the commercial incentives that a coalition could offer, U.S. and allied companies are likely to remain focused on the largest, wealthiest markets, overlooking the developing world.

A group of wealthy democracies with strong common interests could provide a critical mass. Collectively, seven U.S. allies—Australia, Canada, France, Germany, Japan, South Korea, and the United Kingdom—outspend China on R&D. Although the pandemic has clouded their economic prospects, they are still projected to account for roughly a fifth of global GDP in 2030. All these countries are U.S. treaty allies and democracies, but the coalition's mission must extend beyond simply protecting wealthy democracies. It must also engage and support rising hubs on the periphery, large economies in the developing world with a mixture of overlapping and distinct interests.

Two bridges are especially critical to building this coalition. The first bridge stretches across the Atlantic. Despite common values, the United States and Europe look at global networks differently. Lacking a technology champion of similar size, some European leaders view U.S.

technology companies as even more threatening than Chinese companies. The European Union is trying to position itself as a middle option between the open U.S. model and the state-centric Chinese model. Disagreements over data flows and content regulation must be managed through existing mechanisms and new avenues such as the EU-U.S. Trade and Technology Council.

There are real prospects for stronger transatlantic cooperation as well. The United States could remove obstacles to cooperation by adopting national data privacy regulations aligned with the EU's own General Data Protection Regulation, encouraging greater competition in the digital economy, and implementing the OECD global minimum tax agreement. At the International Telecommunication Union, a UN agency, the United States and its European allies should work to elect Doreen Bogdan-Martin as the next director-general and advance socially responsible standards in emerging areas such as AI surveillance, while blocking Chinese proposals to hand governments more control over the internet.

The second bridge extends into the developing world and begins with India, which is expected to become the world's most populous country in the coming years, making it the critical swing state in the global network competition. Realizing India's promise as a growing market and hub for digital services and manufacturing will require breaking its dependency on Chinese hardware. In 2019, India imported about 40 percent of its telecommunications equipment from China and nearly two-thirds of its data center equipment from China and Hong Kong. Three of India's four largest carriers rely on Huawei and ZTE equipment for 30-40 percent of their networks.

Ultimately, India's participation in the coalition should be based on actions, not aspirations. New Delhi is the world's leader in internet shutdowns and has declined to join talks on e-commerce at the World Trade Organization and data flow initiatives at the G20. The coalition should work with India to craft a roadmap for addressing these shortcomings. India's reforms could be incentivized with policies that strengthen its manufacturing sector, diversify supply chains, connect its own citizens, and win customers in foreign markets.

IV. Recommendations

A successful strategy for meeting this global challenge begins at home, but it does not end there. The United States still has its own communities to connect and a digital divide that will widen if left to market forces. It must push forward the frontiers of technology by educating and attracting the next generation of innovators, ensuring they have the resources to succeed and the competitive space for new businesses to flourish. It must fashion data policies that protect citizens' privacy and their security. At the same time, the United States must compete in tomorrow's markets. With that international competition in mind, the recommendations below focus on sharpening U.S. tools, expanding affordable alternatives, and exploiting China's weaknesses.

Sharpen U.S. Tools

1. **Unleash the U.S. International Development Finance Corporation (DFC).** Update budget rules to allow the DFC to make better use of its equity authority, create a position at the DFC for a senior official in charge of ICT investments, and increase the share of digital infrastructure projects in the DFC's portfolio.

2. **Expand the U.S. Commercial Foreign Service** to remove and prevent barriers to U.S. suppliers in key emerging markets. In Africa, for example, China has 10 to 40 government representatives for every U.S. foreign commercial service officer there. This expansion should include a focus on recruiting individuals with technology backgrounds.

3. **Conduct a global networks assessment.** The National Intelligence Council, with input from U.S. agencies and the private sector, should assess key trends and scenarios for telecommunications networks and their implications for U.S. interests over the next decade. An unclassified version of the assessment should be made public.

4. **Update defense commitments to include a greater focus on technology.** The recent AUKUS partnership, which includes a technology sharing dimension, is an encouraging example of updating defense partnerships for the digital age. More should be done to adopt existing tech and invest in future capabilities. For example, NATO members could be permitted to count some spending on critical digital infrastructure with a direct application to NATO communications, such as select 5G systems, toward their overall spending obligations.[9]

Expand Affordable Alternatives

5. **Launch digital pilot projects.** As the U.S. and its allies look to launch pilot projects for the G7's Build Back Better World partnership and related efforts, such as the Blue Dot Network, they should put an emphasis on digital infrastructure projects, which in addition to being important, often cost less and take less time to complete than large transport and energy projects.

6. **Put a price on security.** Provide technical assistance to improve how countries assess costs and reach decisions. The initial price tag on Chinese projects often only includes the up-front costs associated with construction, overlooking maintenance and operations costs. Rather than simply warning against security risks, the economic costs of those risks should be estimated, widely advertised, and factored into cost-benefit analyses.

7. **Pursue a digital trade deal** that pushes back against the rise in data localization policies, supports the responsible use of ICT and emerging technologies such as AI, and lowers barriers to access for small businesses.

8. **Develop a "Sustainable Cities" certification** for cities and companies that emphasizes commercial viability, energy efficiency, social safeguards, and data security. Cities receiving the certification could receive financial and technical assistance. Companies that qualify could receive priority when competing for projects in those cities.

[9] Terry Schultz, interview with Simon Handler and Safa Edwards, NATO 20/2020 Atlantic Council, podcast audio, February 10, 2021, https://www.atlanticcouncil.org/ content-series/nato20-2020/ supersize-cyber-nato-20-2020-podcast/; Lindsey Gorman, "NATO Should Count Spending on Secure 5G Towards Its 2% Goals," Defense One, December 3, 2019, https://www.defenseone.com/ideas/2019/12/ nato-should-count-secure-5g-spending-towards-its-2-goals/161648/.

9. **Create an Open RAN international academy.** Open RAN offers more choice and presents less risk of becoming locked into a single vendor, but it also adds complexity. This effort would train foreign operators and share specifications for tested and trusted combinations of hardware to reduce uncertainty.

10. **Launch a global cloud public-private partnership.** Work with U.S. companies and NGOs to support pilot cloud projects in emerging markets that package services, hard infrastructure, and training opportunities. In addition to building partners' technical capacities and increasing the adoption of trusted services, these projects could be used to incentivize openness to data flows.

11. **Bring LEO broadband to low-income markets.** Help U.S. LEO broadband providers secure landing rights overseas, and work through multilateral development banks to provide financial support for customers in low-income markets to access these services.

Exploit China's Weaknesses

12. **Invest in technologies that challenge authoritarian networks.** Increase funding for the Open Technology Fund (OTF) and other efforts to support tools such as Tor and Signal that help dissidents communicate securely and reconstitute their websites after an attack. More sophisticated tools will also make China's authoritarian approach more expensive to maintain.

13. **Expose false claims.** Chinese companies have left a trail of exaggerations and outright lies about their "safe city" systems, surveillance cameras, data centers, and other products. Technical assistance and public-awareness campaigns that uncover and expose these shortcomings—not just security flaws but also performance shortcomings and broken promises—could help shift the cost-benefit analysis of decisionmakers.

14. **Expand information-sharing.** Much of China's commercial diplomacy is conducted bilaterally and opaquely, which maximizes its negotiating power, limits outside scrutiny, and prevents its partners from sharing information with each other. The United States should encourage countries to adopt laws that require publishing government contracts and create opportunities for developing countries to share information and lessons learned with each other.

15. **Cement first-mover advantages.** China is attempting to match and surpass U.S. digital capabilities, but it remains behind in cloud computing, LEO broadband, and other important areas. Even as U.S. policymakers address areas where the United States lags (e.g., 5G), they must help U.S. workers and companies press these existing advantages through policies that support innovating, expanding into foreign markets, and striking long-term partnership agreements.