`

Testimony Before the U.S.-China Economic and Security Review Commission

By Graham Webster

Senior Fellow, Paul Tsai China Center, Yale Law School
Fellow and Coordinating Editor, DigiChina, New America

Hearing on "U.S. Tools to Address Chinese Market Distortions"

June 8, 2018

Introduction

I'd like to thank the chairs, the entire Commission, and its professional staff for inviting me to speak with you today on the important topic of China's technological development policies. I come to you today as a practitioner of Track 2 and Track 1.5 diplomacy between the United States and China on a wide variety of issues for more than five years with Yale Law School's Paul Tsai China Center, and as coordinating editor of the DigiChina project at New America, a cross-organization collaborative effort to translate, analyze, and contextualize policy developments in China's digital economy. In this written testimony, I cite a great deal of our DigiChina work in recognition that, while my opinions and any errors are my own, I would have precious little to offer without the constructive collaboration over the last year of this community of specialists.

The theme of this hearing is "U.S. tools to address Chinese market distortions," and this panel focuses on exploring "a coordinated policy response to China's technonationalism." Commission staff have written a very useful summary of "China's technonationalism toolbox," naming 10 policy tools Chinese authorities have used in efforts to strengthen their country's technological development.[1] In my testimony today, I will focus especially on one such tool—regulations.

General Principles in Analyzing Chinese Policy Developments

First, before we review the details of Chinese policy developments, there are a few important themes to keep in mind:

[1] Katherine Koleski and Nargiza Salidjanova, "China's Technonationalism Toolbox: A Primer," U.S.-China Economic and Security Review Commission, https://www.uscc.gov/sites/default/files/Research/China%27s%20Technonationalism.pdf.

Chinese government efforts to develop a more independent technology base are broad and deep, and they will not be halted. The Communist Party for years has repeatedly articulated ambitions to enhance China's role in global science and technology development. Leaders have in recent years made clear they view dependencies on certain foreign technologies as potential threats to national security and regime survival. It has been more than five years since Chinese media identified U.S. firms as "eight guardian warriors" with broad and deep presence in China's networks; security-minded Chinese analysts and officials spoke of "secure and controllable" systems in contrast.[2] And speaking from first-hand experience in bilateral dialogues, it is clear the Snowden revelations only intensified this concern.

This adversarial-minded security motivation for seeking sharply reduced levels of technological dependence is accompanied by a genuine desire to guide and encourage economic development in a direction that improves people's lives, moves the economy up the global value chain, and gives Chinese citizens a steady stream of accomplishments to be proud of. Together, the security and development motivations for "indigenous innovation" in "core technologies" constitute a force that cannot be stopped entirely.[3] Seeking a total halt to this process would be akin to fighting gravity. Instead, responses should assume that this gravitational force will persist, but that the way it acts in the world can be shaped through incentives, institutional design, and technological innovation itself.

Chinese plans express ambitions, but not always expected realities. In China's system, government plans provide guidance and set the direction of work across the bureaucracy and for some market actors. The 2017 New Generation Artificial Intelligence Development Plan (AIDP) is an example of a document full of aspirations but drafted in full awareness that technological or market developments may change the definition of success.[4] Anyone seeking to understand the likely course of events should be aware of plans and ambitions but spend more time focusing on concrete events and achievements. Even programs, such as Made in China 2025 (MIC2025), that channel funding and set domestic content targets are limited by realities of the status quo of China's industrial development.

Formal Chinese laws and regulations operate in parallel with more opaque politics. Understanding the realities of China's digital economy regulatory environment requires attention to laws and other regulatory instruments, both before and after they become final. The full story, however, lies in how those documents combine with realities of enforcement (or not) and informal arrangements market participants may reach with regulators. Firms and governments may reach understandings with officials that reduce regulatory ambiguity or circumvent troublesome barriers, but this informal layer of governance increases uncertainty and volatility in

[2] Even before the Snowden revelations, commentators had identified the eight (Cisco, IBM, Google, Qualcomm, Intel, Apple, Oracle, and Microsoft), and a "de-Ciscoization" campaign was being discussed. See Graham Webster, "China and the Eight Guardian Warriors of American Tech," *SupChina*, https://supchina.com/2017/03/16/china-eight-guardian-warriors-tech/.

[3] Paul Triolo et al., "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," *DigiChina* (2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

[4] Graham Webster et al., "China's Plan to 'Lead' in Ai: Purpose, Prospects, and Problems," ibid. (2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/.

the regulatory environment writ large. Successful international business or political responses will respond to both black-and-white and gray areas in the policy environment.

Regulators and the central leadership in China are responsive to international events, including U.S. behavior. Though the basic goals of spurring indigenous innovation and a degree of technological independence will not fade, Chinese officials adjust to the international environment in both positive and negative ways. A positive story might be the relatively strong influence Europe's General Data Protection Regulation (GDPR) has had on China's emerging data protection regime. The EU's GDPR-based global agenda-setting power has been strong, and Chinese thinkers and officials have grasped an opportunity to make their digital economy more interoperable. A negative story of influence might be the Commerce Department decision (under review at time of writing) to deny the Chinese information and communications technology (ICT) company ZTE access to U.S. components.[5] Having demonstrated a capability and willingness to cut off a major company from crucial suppliers, the U.S. government reinforced Chinese views that domestically-produced and -designed ICT components must be developed, and that the United States is a potentially unreliable partner in critical technology sectors.

The Chinese government is far from monolithic. While it is well established that divisions exist within China's authoritarian government, certain divides are crucial for understanding the regulations that shape the digital economy. There, a perennial tension exists between officials and offices responsible for security and those responsible for technological and economic development. Major Chinese ICT companies also have clout in certain areas of regulation, and they are rarely perfectly aligned with their regulators. The give-and-take among power centers can highlight areas of flexibility.

Chinese Policies That Pose Challenges for International Companies

The Chinese government's digital technology approach can be understood as having three crucial layers: national ambitions, development plans and initiatives, and policies. Each layer contains elements that have implications for international (especially U.S.) competition, and elements that are influenced by international (especially U.S.) behavior.

Layer I: National Ambitions.

Under Xi Jinping, officials describe the central national ambition in digital technology as a strategy of building China into a "cyber superpower" or "cyber great power."[6] An authoritative September 2017 article published in the Party journal *Qiushi* describes China's "cyber superpower" strategy as operating in four major areas: (1) online content management, including propaganda and censorship; (2) ensuring cybersecurity, broadly conceived; (3) building a

[5] Graham Webster, "China's Zte Has Long Been on Washington's Radar, for Quite a Few Reasons. Here's the Story.," *Washington Post* (2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/22/chinas-zte-has-long-been-on-washingtons-radar-for-quite-a-few-reasons-heres-the-story/?utm_term=.c7af6a5a88bd.

[6] Rogier Creemers et al., "Lexicon: 网络强国 Wǎngluò Qiángguó: Understanding and Translating a Crucial Slogan and 'Cyber Superpower' Ambition," *DigiChina*, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

domestic development and production base for Internet technologies; (4) and increasing Chinese influence on the governance and development of the global Internet.[7]

(1) Online content management is primarily a domestic concern, but the uncensored global Internet and proactive U.S. and international efforts to advance freedom of speech are directly in tension with this goal.

(2) Ensuring cybersecurity is a comprehensive goal, the achievement of which requires efforts by domestic Chinese actors and creates a range of processes designed to ensure national security, personal privacy, broader data protection, and network security. While there are significant domestic elements of this goal, including data protection practices and standards for procurement in sensitive systems, the cybersecurity goal directly interacts with global markets. Consciousness of cybersecurity risks rose significantly in China following the Snowden revelations, and U.S. intelligence services are often cited as adversaries against which Chinese entities should defend. Even without specific reference to U.S. spying, the task of increasing cybersecurity standards could be expected to bring about regimes to review and certify hardware and software—and such regimes can be used to limit international competition either through manipulating processes or because uncertainty about reviews adds friction to the market.

(3) The drive for "indigenous innovation" in "core technologies"—by no means limited to the digital world—arises from a hybrid motivation. Chinese leaders have good reason to encourage the economy to climb the value chain. Heavy industry and low-tech manufacturing are unsustainable for China for reasons such as rising wages, environmental impacts, and social inequalities. Hence MIC2025 seeks to develop world-leading industries in high-tech sectors. Meanwhile, at a time when market and national security tensions are heightened, China's economy also risks significant disruption if it remains heavily dependent on foreign components or intellectual property. Actions like the ZTE denial order further underline the leverage foreign governments may have over domestic industrial production and economic advancement. That amount of leverage is unacceptable to Chinese leaders, and so part of seeking to build China into a "cyber superpower" is ensuring a more independent ICT stack.

(4) Efforts to increase China's influence over the development and governance of the Internet globally have two main motivations. First, they advocate for the supremacy of state actors in governing the Internet, pushing a "multilateral" model of Internet governance, as opposed to the "multi-stakeholder" status quo historically favored by the U.S. government. Second, Chinese officials seek an increased role for Chinese companies

[7] Analysis and translation: Paul Triolo et al., "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated," ibid., https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/. Chinese-language original: 中央网信办理论学习中心组 [Cyberspace Administration of China Theoretical Studies Center Group], "深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作 [Deepening the Implementation of General Secretary Xi Jinping's Strategic Thinking on Building China into a Cyber Superpower: Steadily Advancing Cybersecurity and Informatization Work]," *求是 [Qiushi]*, Sept. 15.

in building out the Internet across the world, especially in developing countries, and especially in the countries connected with Belt and Road Initiative rhetoric or the related Digital Silk Road concept.

The framing for the Chinese government's "cyber superpower" or "cyber great power" ambition implicitly sets a goal of reaching general parity with any other national power in digital technology, and that means at minimum rising to become a near peer of the United States. Such an ambition is no simple task, especially in a country where overall Internet penetration only recently surpassed 50 percent, reaching 55.8 percent in December 2017, according to official statistics.[8]

Layer II: Development Plans and Initiatives.

Although China's economy has transformed dramatically since Reform and Opening, the party-state retains the practices of long-term planning and top-down development strategizing. U.S. and other governments have devoted considerable attention to such plans and strategies in recent years, especially Made in China 2025 (MIC2025) and the New Generation Artificial Intelligence Development Plan (AIDP).

In both cases, and in other industrial planning or development funding initiatives such as the National Integrated Circuit Industry Investment Fund (IC Fund), Chinese companies and researchers often significantly lag global leaders. Challenges ranging from talent cultivation to intellectual property development and mastering specialized manufacturing techniques will not be surmounted easily. Even as some innovation efforts take off, others are likely to remain mired in such foundational challenges.

International reporting on Chinese development plans and initiatives often cites eye-popping targets for market development, loans, or research and development (R&D) funding. Big numbers may be misleading, however: Top-down R&D may be less efficient than market-based efforts around the world, and targets in high-tech fields more than a few years out are unlikely to be rooted in realistic assessments of what's possible.

Official Chinese plans and initiatives are important as unifying principles around which already existing and newly encouraged efforts can rally, but their effects on concrete industry developments must be examined empirically, and efforts to mitigate ill effects stand a better chance of success if they focus on outcomes instead of slogans. When plans like MIC2025 or the AIDP become highly visible symbols, it becomes increasingly likely that foreign pressure to roll back the efforts will instead produce a reflexive firming of public resolve.

Layer III: Policies.

For international business, the policy environment is one area where China's official ambitions and plans become pervasively relevant. Since Xi Jinping became the top leader, the Chinese

[8] "第 41 次《中国互联网络发展状况统计报告》[the 41st "China Internet Development Conditions Statistical Report"]," http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/t20180305_70249.htm.

government has advanced a perhaps uniquely comprehensive effort to construct a cohesive policy environment for cyberspace.

In kicking off this process, the Xi administration took the consequential step in 2014 of establishing the Central Leading Group for Cybersecurity and Informatization (CLGCI) chaired by Xi himself, which centralized decision-making on cyberspace and ICT policy. The CLGCI secretariat, the Cyberspace Administration of China (CAC), then advanced efforts to coordinate and produce policy frameworks for which responsibility had previously been spread across several bureaucracies—including the Ministry of Public Security (MPS), the Ministry of Industry and Information Technology (MIIT), the Ministry of Propaganda, and the military and intelligence establishments.

CAC's role was further elevated this year when the State Council announced that the CLGCI would be upgraded from "central leading group" to "central commission" status. The renamed Central Commission for Cybersecurity and Informatization (CCCI) retained CAC as its secretariat.[9] (Formally, CAC is a "one structure, two nameplates" entity serving as the secretariat of the Party's CCCI and as the State Internet Information Office.) Although the full membership of the CCCI is not yet public, official coverage of an important Xi speech at an April National Cybersecurity and Informatization Work Conference named Premier Li Keqiang and Politburo Standing Committee Member Wang Huning, a close Xi adviser, as vice chairs.[10]

The interagency process centralized in CAC has produced an array of regulatory developments with the Cybersecurity Law (published in late 2016 and in effect since June 1, 2017) at its center. Other laws, including the National Security Law, the Counterterrorism Law, the National Intelligence Law, and a pending Encryption Law, interlock with this framework. We can understand the Cybersecurity Law and related regulatory efforts as an interlocking matrix of six regulatory systems. Here I briefly summarize the framework described by our joint work from New America's DigiChina project.[11] For international business, the most consequential elements of the Cybersecurity Law framework are emphasized in bold.

- *The Internet Information Content Management System.*
  This system tightens controls over online activities, attaching activity to users' offline identities. It censors information the government views as harmful and **imposes "self-regulation" on intermediaries**.

- *The Cybersecurity Multi-Level Protection System (MLPS).*
  This preexisting system, launched in 2006 and associated with MPS efforts to secure critical infrastructure, ranks network applications by sensitivity, imposes security

[9] Rogier Creemers et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization," *DigiChina*, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.
[10] Paul Triolo et al., "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," ibid., https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.
[11] Paul Triolo et al., "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework," ibid., https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

requirements, and **issues certifications** accordingly.

- *The Critical Information Infrastructure Security Protection System.*
  The **concept of "critical information infrastructure" (CII)** is a crucial element of the Cybersecurity Law framework. It overlaps with but is broader than classical concepts of critical infrastructure, and operators of CII are subject to security reviews for procurement, data protection requirements, and other regulation.

- *The Personal Information and Important Data Protection System.*
  The Cybersecurity Law and related regulatory documents outline new protections for "**personal information**" and "**important data**," though neither of these concepts is fully defined. **Cross-border data transfer** and **data localization** requirements emerge here and in the CII system, and some elements of this system are self-consciously designed to maximize interoperability with international regimes such as GDPR.

- *Network Products and Services Management System.*
  This still-nascent system encompasses the **Cybersecurity review regime** (CRR) to undertake reviews of products and services used by CII operators. The scope and standards of review are not yet clear. The system's interaction with the existing MLPS is not clear either.

- *The Cybersecurity Incident Management System.*
  Incident response, threat information sharing, and standards-setting are all increasingly centralized under the CAC, which in April took over from MIIT as parent of the National Computer Network and Information Security Management Center (NCNISMC), "which is closely associated or essentially conterminous with the National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC)," according to our analysis.[12]

How China's Digital Regulatory Environment Affects International Companies

These schematic systems pose several challenges for international companies, and indeed for Chinese companies as well. Some are best viewed from the perspective of network operators' obligations, and others are best viewed through the lens of data collection, storage, and movement. In all cases, the regulations create significant uncertainty.[13]

Obligations for Network Operators (and Their Suppliers)

[12] Rogier Creemers et al., "China's Cyberspace Authorities Set to Gain Clout in Reorganization," ibid., https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

[13] In testimony before a House subcommittee, Samm Sacks of the Center for Strategic and International Studies offers an alternative helpful way to understand impacts on international companies, identifying several different kinds of review regimes, plus a drive for localization. See House Energy and Commerce Subcommittee on Communications and Technology, *Telecommunications, Global Competitiveness, and National Security*, May 16. https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-Wstate-SacksS-20180516-U21.pdf

Entities that operate networks in China potentially face several different challenges. First, if they are operating "critical information infrastructure" (CII), a concept central to the Cybersecurity Law, products and services they use must undergo review in a still-nascent "cybersecurity review regime" (CRR).

CII is not well defined. In the Cybersecurity Law, CII specifically includes "public communication and information services, power, traffic, water resources, finance, public service, and e-government." In draft regulations from July 2017, "sectors such as media, specifically including radio stations, television stations, news agencies, and other such news work units" plus sanitation, healthcare, cloud computing, and big data are all marked as CII.[14] Article 19 of the draft regulations further gives sectoral regulators responsibility (and apparently discretion) to define CII in their area of work. The theoretically possible reach of the CII category is practically limitless, so until further regulations or standards clarify its boundaries, foreign entities acting either as suppliers to or operators of potential CII will not clearly know their obligations.

The CRR is not fully set up. Questions remain about the cybersecurity reviews that products fueling CII would be required to pass. Among them: What standards for security will be employed? Who will do the examining? (Although some of the examiners have been identified, a full decision-making process is not yet clear.) Will previous certifications, for instance under MLPS, suffice or smooth processes? Will informal approvals negotiated with regulators stick?

The question of whether prior arrangements will hold was exemplified in the public sphere in June 2017 when controversy erupted over Microsoft's Windows 10 China Government Edition, produced in cooperation with China Electronics Technology Group Corporation (CETC). For such a general purpose product as an operating system—and for a variant designed specifically to serve public sector customers—it is fairly clear that CII operators would need an option that satisfies the CRR requirements. Thus several days after the Cybersecurity Law went into effect, Chinese Academy of Engineering Academician Ni Guangnan, long an advocate for development of an indigenous Chinese operating system, called for a halt of purchases of the Windows 10 China Government Edition by government customers. Ni rejected the "user testing" and "security testing" the Microsoft-CETC product had undergone before the Cybersecurity Law took effect and called for a new cybersecurity review. Ni expressed the opinion that the new review would "at minimum require[] access to the software's refactorable and complete source code."[15]

Halting the progress of a product designed specifically to address Chinese government security concerns for software running in the public sector would be extraordinary, and Ni's view that full source code examination would be necessary would imply the possibility of intellectual property loss during the review. But Ni's wasn't the only influential voice here. A few days later, Wang Jun, a lead engineer from the China Information Technology Security Evaluation Center

[14] Paul Triolo, Rogier Creemers, and Graham Webster, "China's Ambitious Rules to Secure 'Critical Information Infrastructure'," *DigiChina*, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.

[15] Graham Webster, "Ni Guangnan: China Should Suspend Purchases and Use of Windows 10 China Government Edition Pending Security Review (Translation)," *Transpacifica*, http://transpacifica.net/2017/06/ni-guangnan-china-should-suspend-purchases-and-use-of-windows-10-chinese-government-edition-pending-security-review-translation/.

(CNITSEC, a pseudo-governmental organization likely to be involved in the CRR), credited the Microsoft approach and pushed back on Ni's firm view. "According to my understanding, in their cooperation, Microsoft is willing to open source code under the condition that intellectual property is protected. I believe developing Windows 10 or another later government-use edition in this method is a positive and meaningful attempt," Wang said. "We understand the goal of this method is to try to give government and critical information infrastructure users an improved edition that suits Chinese users' security requirements better than the general edition." Wang's broader interview advocated for prudent security review measures and implicitly against strict application of rules in a case such as this.[16]

Obligations for Those Handling 'Important' or 'Personal' Data

Data localization and cross-border transfer. The Cybersecurity Law may seem to make some things clear. "Personal information and other important data gathered or produced by CII operators during operations within the mainland territory of the People's Republic of China shall be stored within mainland China" (Article 37). Even allowing for the ambiguity in definitions for CII, personal information (PI), and important data (ID), the requirement to store significant categories of data is clear. Article 37 further provides that a "security assessment" is required before transferring these classes of data out of mainland China. If a foreign entity is deemed to be operating CII and collecting or producing PI or ID, it would have to follow these rules.

In September, the U.S. government filed a WTO challenge to this cross-border data transfer review regime, saying: "The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates."[17] In response, a Chinese government social media account released a short statement stating that two key regulatory documents that color in details of the regime on cross-border data transfer were still under revision, and "the controversy and compromise has not yet been resolved, which will continue to test the technological and coordinating capabilities of the legislature." Having acknowledged that the Cybersecurity Law, formally in effect, did not specify all of the answers, the posting continued: "it is foreseeable that various stakeholders in the game will persist in the tendency to make interpretations." The implication was that lobbying about the details of implementation had not concluded.[18] By all appearances, approximately nine months later, this is still the case.

Protecting personal information. Articles 41–45 outline requirements for handling of PI by the broader category of "network operators," and those requirements are fleshed out in considerable detail in a nonbinding but authoritative document issued by the CAC-subordinate Technical Committee 260 (TC260) standards setting body, the Personal Information Security Specification.

---

[16] Rogier Creemers, Paul Triolo, and Graham Webster, "Chinese It Security Examiner Describes Review Process, Clarifies Status of Chinese Government Windows Edition," ibid., http://transpacifica.net/2017/06/1963/.

[17] "Communication from the United States: Measures Adopted and under Development by China Relating to Its Cybersecurity Law," (World Trade Organization). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf

[18] Samm Sacks, Paul Triolo, and Graham Webster, "Beyond the Worst-Case Assumptions on China's Cybersecurity Law: There's Still an Internal Tug-of-War over Cross-Border Data Flows," *DigiChina*, https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/.

A more detailed but still nonbinding definition of "personal information" is provided in the Specification. International businesses are even more likely to be deemed "network operators" than CII operators, and this data protection regime places significant though not internationally unusual compliance requirements on those handling personal information.

Common Themes

Across several areas of regulation, there are common themes.

- First, important concepts that determine who is subject to what kind of regulation are often only partially defined. These include CII, important data, and personal information.

- Second, where there is ambiguity, there is discretion. While definitions are still being clarified, regulators can use the ambiguity to help or hurt whoever they choose, an obvious potential avenue for political influence on outcomes.

- Third, in each area of regulation, the government pursues interests broadly seen as legitimate (for example in security, personal privacy protection, or ensuring reliable operation of networks) while also pursuing goals opposed by the U.S. government (for example favoring domestic businesses, targeting dissidents, or restricting speech).

Tools and Recommendations for the U.S. Government

There are a number of measures the U.S. government should consider taking in advocating for the American people in the face of Chinese digital technology regulations.

- Some of China's regulations or practices may be in tension with or directly in violation of WTO disciplines. The U.S. government should use available WTO tools to pursue remedies. U.S. government should also support efforts to improve the WTO system along with allies that share the interests of the American people. It must be said, however, that if the U.S. government wishes to employ elements of the established, rules-based international trade order, it should refrain from offering dubious national security justifications for tariffs or other restrictions on foreign trade. U.S. claims that lack strong justification undermine efforts to exert pressure on China.

- The U.S. government and industry groups seeking leverage against Chinese practices that harm their competitiveness should coordinate international trade actions, standards for national security review in investments, and advocacy on ongoing policy developments within China. The U.S. government should refrain from actions that unnecessarily antagonize allied governments or industry groups.

- The U.S. government should keep objectives clear and transparent when developing or revising systems that can limit Chinese investments or acquisitions in the United States. Measures described in terms of protecting U.S. national security should have clear and credible connections to national security. U.S. government credibility is threatened when

measures that have visible commercial benefits for U.S. interests are justified in vague terms of national security.

- National security-related reviews on the part of the U.S. government should be as transparent as possible so as to minimize the appearance or actuality of conflict of interest. U.S. advocacy against opaque Chinese review practices is far less credible when U.S. actions themselves appear to discriminate based on national origin, not only based on bona fide national security concerns.

- Congress should work proactively to channel more resources to fundamental research and innovation in technology fields in the United States. The U.S. government should ensure that the United States remains an attractive place to study, conduct research, and build businesses that provide economic and social benefits.

- The U.S. government should police practices, not peoples. If the United States targets a nationality for increased scrutiny, it surrenders the mantle of the American dream and descends into ugly suspicion. Overreliance on national origin as a risk factor can also increase the likelihood that risks from less-scrutinized countries may go undetected.

- The United States should become a leader in the development of digital technologies that are protective of human rights, such as privacy and freedom of expression, by their design. For example, in the era of artificial intelligence applications based on large datasets about people, the United States has the potential to consistently lead Chinese competitors in developing systems that respect fundamental rights and operate ethically. But industry may not be motivated to do this itself. This means the government should develop regulatory incentives in the United States that better protect U.S. citizens' data and incentivize U.S. businesses to develop world-leading rights-protecting technologies.

- The Executive Branch should ensure, and Congress should demand, that law enforcement actions in the trade sphere remain independent of political agendas. It undermines U.S. democratic norms and the legitimacy of U.S. law if one can reasonably suspect that a law enforcement action—be it an indictment of alleged Chinese military hackers or a denial order in a sanctions case—is a chip on the negotiating table and not an impartial function of the U.S. government.

It should be needless to say, but in today's political climate it needs to be said: Not every Chinese achievement is a U.S. loss, and not every Chinese technological product comes from purloined intellectual property. The peoples of the United States and China are going to have to live with each other as neighbors across an oft-traversed Pacific, and as competitors in a variety of fields. They will live with each other as potential adversaries in some spheres, but also as fellow human beings facing common challenges such as climate change, rising inequality, and threats to international security.

The United States should authentically stand for the openness the Chinese government has recently (and somewhat disingenuously) claimed as its approach in cyberspace. I hope the United States will continue to rise to its highest aspirations as a land where people dreaming of a better

life are met with open arms, courtesy everywhere from border checkpoints to campus communities, and a nation proud to welcome visitors and claim new Americans as compatriots.

Works Cited

"Communication from the United States: Measures Adopted and under Development by China Relating to Its Cybersecurity Law." World Trade Organization, 2017.

Creemers, Rogier, Paul Triolo, Samm Sacks, Xiaomeng Lu, and Graham Webster. "China's Cyberspace Authorities Set to Gain Clout in Reorganization." *DigiChina* (2018). https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

Creemers, Rogier, Paul Triolo, and Graham Webster. "Chinese It Security Examiner Describes Review Process, Clarifies Status of Chinese Government Windows Edition." *Transpacifica* (2017). http://transpacifica.net/2017/06/1963/.

Creemers, Rogier, Graham Webster, Paul Triolo, Katherine Tai, Lorand Laskai, and Abigail Coplin. "Lexicon: 网络强国 Wǎngluò Qiángguó: Understanding and Translating a Crucial Slogan and 'Cyber Superpower' Ambition." *DigiChina* (2018). https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

Koleski, Katherine, and Nargiza Salidjanova. "China's Technonationalism Toolbox: A Primer." U.S.-China Economic and Security Review Commission, https://www.uscc.gov/sites/default/files/Research/China%27s Technonationalism.pdf.

House Energy and Commerce Subcommittee on Communications and Technology. *Telecommunications, Global Competitiveness, and National Security*, May 16 2018.

Sacks, Samm, Paul Triolo, and Graham Webster. "Beyond the Worst-Case Assumptions on China's Cybersecurity Law: There's Still an Internal Tug-of-War over Cross-Border Data Flows." *DigiChina* (2017). https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/.

Triolo, Paul, Rogier Creemers, and Graham Webster. "China's Ambitious Rules to Secure 'Critical Information Infrastructure'." *DigiChina* (2017). https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.

Triolo, Paul, Lorand Laskai, Graham Webster, and Katherine Tai. "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities." *DigiChina* (2018). https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

Triolo, Paul, Samm Sacks, Graham Webster, and Rogier Creemers. "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework." *DigiChina* (2017). https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

Triolo, Paul, Graham Webster, Samm Sacks, and Elsa Kania. "China's Strategic Thinking on Building Power in Cyberspace: A Top Party Journal's Timely Explanation Translated." *DigiChina* (2017). Published electronically Sept. 25. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

Webster, Graham. "China and the Eight Guardian Warriors of American Tech." *SupChina* (2017). https://supchina.com/2017/03/16/china-eight-guardian-warriors-tech/.

———. "China's Zte Has Long Been on Washington's Radar, for Quite a Few Reasons. Here's the Story." *Washington Post* (2018). https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/22/chinas-zte-has-long-been-on-washingtons-radar-for-quite-a-few-reasons-heres-the-story/?utm_term=.c7af6a5a88bd.

———. "Ni Guangnan: China Should Suspend Purchases and Use of Windows 10 China Government Edition Pending Security Review (Translation)." *Transpacifica* (2017). http://transpacifica.net/2017/06/ni-guangnan-china-should-suspend-purchases-and-use-of-windows-10-chinese-government-edition-pending-security-review-translation/.

Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. "China's Plan to 'Lead' in Ai: Purpose, Prospects, and Problems." *DigiChina* (2017). https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/.

中央网信办理论学习中心组 [Cyberspace Administration of China Theoretical Studies Center Group]. "深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作 [Deepening the Implementation of General Secretary Xi Jinping's Strategic Thinking on Building China into a Cyber Superpower: Steadily Advancing Cybersecurity and Informatization Work]." *求是 [Qiushi]*, Sept. 15 2017.

"第 41 次《中国互联网络发展状况统计报告》[the 41st "China Internet Development Conditions Statistical Report"]." Published electronically March 5. http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/t20180305_70249.htm.