A HOOVER INSTITUTION ESSAY

Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses

MEI GECHLIK

Aegis Series Paper No. 1706

Introduction

After Chinese President Xi Jinping's visit to the United States in September 2015, the two countries announced that they "are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community."[1] They also agreed "to create a senior experts group for further discussions on this topic." In May 2016, such a group held its first meeting and reportedly had "positive, in-depth and constructive" discussions, but details about these discussions remain unclear.[2]

What is clear, however, is that China has reiterated the importance of discussing appropriate norms of state behavior in cyberspace by focusing on the International Code of Conduct for Information Security that it, together with Russia and a few other member states of the Shanghai Cooperation Organization (SCO), submitted to the General Assembly of the United Nations in January 2015.[3] The Code has, as explained below, aroused concerns among stakeholders in the United States and the international human rights community.

Finding cybernorms that are acceptable to the United States and China, which have different ideologies and practices as well as enormous interests at stake, is obviously not easy. However, recent developments in China show that paragraphs 2(7) and 2(8) of the Code present new opportunities for the two countries to reach a measure of consensus

A draft of this article was presented at the *Conference on US-China Relations: Cyber and Technology* held by the National Security, Technology, and Law Working Group of the Hoover Institution, March 14–15, 2017, at Stanford University. Drawing on this piece, Professor Gechlik shared her thoughts about US-China cyber relations and related implications for businesses and governance in China at a panel titled *Status of Implications of Chinese Rule Making Under the New Chinese Cybersecurity Law, Is There a Viable Market for Cyber Companies?* of the IT Security Entrepreneurs Forum organized by the Security Innovation Network on March 29, 2017, and also at National Taiwan University on June 20, 2017. The author thanks Dimitri Phillips, Jennifer Ingram, Sean Webb, Di Dai, and Trey Levy for their research and/or editorial assistance.

on setting appropriate norms of state behavior in cyberspace. These two provisions propose:

- Paragraph 2(7): To recognize that the rights of an individual in the offline environment must also be protected in the online environment.

- Paragraph 2(8): All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent, and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, *facilitate access for all* and ensure the stable and secure functioning of the Internet. (emphasis added)

This essay identifies developments that reinforce these provisions and discusses how they, together with the SCO's growing significance in the international arena, call for more strategic thinking among US policymakers so that the United States can seize the new opportunities to engage meaningfully with China in setting cybernorms.

The Code

The Code was first submitted to the UN General Assembly for consideration in September 2011 by China, Russia, Tajikistan, and Uzbekistan. It was then revised and resubmitted in January 2015 by these countries as well as Kazakhstan and Kyrgyzstan (i.e., the six founding member states of the SCO). The SCO's expansion and China's increasing influence inside the organization demand a closer examination of the Code.

What Is the Code?

Paragraph 1 of the Code explains its purpose and scope:[4]

> The purpose of the present code of conduct is to identify the rights and responsibilities of States in the information space, promote constructive and responsible behavior on their part and enhance their cooperation in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open and founded on cooperation, and to ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security.

Paragraph 2 of the Code then lists the thirteen-provision code of conduct which each state subscribing to the document would pledge to follow. Paragraphs 2(7) and 2(8) are two of these thirteen provisions.

China has been emphasizing the importance of the Code. Two examples are illustrative. First, at the thematic discussion on information and cybersecurity at the First Committee of the Seventy-first Session of the UN General Assembly held in October 2016, the Chinese delegation explained:[5]

> The formulation of norms of state behavior is an important step to regulate activities and promote confidence in cyberspace, and therefore should be our priority. As the most authoritative and representative international organization, the UN plays an indispensable role in this regard. China and Russia have submitted an *International Code of Conduct for Information Security* to the General Assembly. The process of UN Group of Government Experts (UNGGE) on Information Security has made continuous progress. Based on those efforts, the international society should discuss in depth relevant norms and work out concrete measures in the areas of the protection of critical infrastructure and fighting against cybercrime and cyber terrorism, with a view to build comprehensive and practical norms for cyberspace at an early date.

Second, on March 1, 2017, China released the International Strategy of Cooperation on Cyberspace to "guide China's participation in international exchange and cooperation in cyberspace for the next period of time."[6] In this document, China enumerates four basic principles,[7] six strategic goals,[8] and a plan of action that covers nine tasks, including developing "rule-based order in cyberspace."[9] Specifically, the document states:[10]

> As the United Nations should play a key role in formulating international rules in cyberspace, China supports the UN General Assembly to adopt resolutions regarding information and cyber security and will continue to facilitate and participate in the processes of the United Nations Governmental Groups of Experts (UNGGE) and other mechanisms.
>
> In January 2015, Shanghai Cooperation Organization (SCO) member states submitted to the UN General Assembly the updated *International Code of Conduct for Information Security*. It is the first international paper dedicated to norms of behavior in cyberspace and an important public security product China and other SCO member states provide to support international efforts for a code of conduct in cyberspace. China will continue to enhance international dialogue to seek broader international understanding and support for this initiative.

The United States and other countries in the West look at the Code quite differently. Although the Code was referenced in the July 2015 report of the UNGGE in the "Field of Information and Telecommunications in the Context of International Security," which addresses norms of behavior and other crucial issues for international security in cyberspace,[11] some of the provisions in the Code have raised concerns in the West that the six founding member states of the SCO are attempting to use the Code to weaken the

preeminent role of the United States in cyber governance[12] and redefine the application of international human rights law by extending national sovereignty and control to cyberspace.[13]

The Code Matters

Despite the above-mentioned concerns about the Code, the document should not be dismissed in any serious discussion of US-China cyber relations because China is likely to continue exerting its influence inside the expanding SCO to garner more support for the Code.

According to the charter of the SCO, which entered into force in 2003, the SCO's main goals include "to consolidate multidisciplinary cooperation in the maintenance and strengthening of *peace, security and stability* in the region," "to jointly *counteract terrorism, separatism and extremism* in all their manifestations," and "to encourage the efficient *regional cooperation* in such spheres as politics, *trade and economy,* defense, law enforcement, environment protection, . . . and also other spheres of common interest" (emphasis added).[14]

Critics in the West look at the SCO's goals with skepticism and believe that the organization is a Russian-Chinese geopolitical device to counter the presence of the United States in central Asia.[15] Nevertheless, the significance of the SCO has been increasing. In December 2004, it was granted observer status in the UN General Assembly. It has also established relations with the Commonwealth of Independent States (2005), the Association of Southeast Asian Nations (2005), the Collective Security Treaty Organization (2007), the Economic Cooperation Organization (2007), the United Nations Office on Drugs and Crime (2011), the Conference on Interaction and Confidence-Building Measures in Asia (2014), and the UN Economic and Social Commission for Asia and the Pacific (2015).[16]

The security goals, especially the fight against terrorism, separatism, and extremism, are, as pointed out by China, among the SCO's priorities.[17] This is reflected in the signing of the Shanghai Convention on Combating Terrorism, Separatism and Extremism on June 15, 2001, when the SCO was founded. The Shanghai Convention defines terrorism, separatism, and extremism and outlines specific principles of the concerted fight against them, helping to lay a legal foundation for security cooperation.[18] Given that modern threats to security also exist in cyberspace, cybersecurity should be a key topic addressed in the SCO's discussion of security issues.

The achievement of these security goals has appeared more promising since June 2017, when India and Pakistan became SCO member states. Covering three-fifths of Eurasia and representing nearly half the world's population,[19] the SCO has amassed enormous

clout to support its international agenda. The SCO's power is likely to grow as the four observer states (Afghanistan, Belarus, Iran, and Mongolia) and six dialogue partners (Azerbaijan, Armenia, Cambodia, Nepal, Turkey, and Sri Lanka) may follow the footsteps of India and Pakistan (both of which were first granted observer status in 2005) to become members of the SCO.[20]

Within the expanding SCO, China is likely to increase its influence through its Belt and Road Initiative (China's going-global plan that has expanded to embrace nearly one hundred countries).[21] Economic cooperation is a key goal for the SCO (e.g., the signing in 2001 of the Memorandum between the Governments of the Member States of the Shanghai Cooperation Organization on the Basic Objectives and Orientation of Regional Economic Cooperation and the Launching of a Process of Trade and Investment Facilitation).[22] With this in mind, Beijing has pledged billions for Belt and Road projects in SCO member states (e.g., the China-Pakistan Economic Corridor). Because China took over the rotating chair of the SCO in June 2017 and is scheduled to host the next annual summit in June 2018,[23] the coming year will likely see China garner more support for its agenda, including the Code, among developing countries. Such countries, which often see opportunities for economic development in a more open Internet but fear exposure to cybersecurity risks, can be expected to find the Code appealing.

If the United States wants to influence the conduct of China (and Russia) in establishing international norms for cyberspace, it may at this point achieve its end more effectively and efficiently by engaging with the Code than by dismissing it and taking up another approach that is unlikely to win support from China and its allies. The remainder of this article explains how this engagement can be achieved.

Related Developments in China

This section examines recent developments in China—better protection of online and offline rights by the new Guiding Cases System as well as foreign and domestic developments regarding facilitation of everyone's access to cyberspace—to show how paragraphs 2(7) and 2(8) of the Code present opportunities for China and the United States to bridge certain gaps in the setting of cybernorms.

Online and Offline Rights

Paragraph 2(7) of the Code requires each state subscribing to the document (including China) "to recognize that the rights of an individual in the offline environment must also be protected in the online environment." As explained in this subsection, China's new Guiding Cases System can help the country give real meaning to this provision by providing a mechanism that ensures that transparency and consistency are achieved in the application of the Cybersecurity Law and related legal matters, such as intellectual property.

The addition of paragraph 2(7) to the 2015 version of the Code can be traced to a finding in a report of the aforementioned UNGGE, whose formation Russia had called for: "existing international law and in particular the United Nations Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [Internet communication technology] environment."[24] In fact, this concept—in language much like that of the Code's paragraph 2(7)—has been frequently referenced within the UN system.[25] Importantly, in the resolution titled The Right to Privacy in the Digital Age adopted by the UN General Assembly on December 18, 2013, the General Assembly "affirms that the same rights that people have offline must also be protected online, including the right to privacy."[26]

The pledge to recognize that the rights of an individual must be equally protected in both offline and online environments should be applauded if the protection in the offline environment has been satisfactory. Given the deficiencies in the Chinese legal system, including inadequate transparency and consistency in the application of law, this pledge made by China understandably leads to concerns (e.g., that it is meant as leeway for the country to provide weak protection of individuals' rights online). Nevertheless, it is worth noting that a breakthrough in the Chinese legal system that began a few years ago has gradually gained momentum and has the potential to ameliorate these deficiencies, thereby giving teeth to this pledge.

In November 2010, as a judicial reform measure in a country which has traditionally focused on statutes and whose judges have been generally criticized for inadequate competency, transparency, and independence, China's Supreme People's Court (SPC) established a groundbreaking system to "summarize adjudication experiences, unify the application of law, enhance adjudication quality, and safeguard judicial impartiality."[27] It announced that certain Chinese court cases were to be selected from different levels of courts located in different regions and reissued as "guiding cases" (GCs) endowed with de facto binding effect, i.e., judges adjudicating similar subsequent cases are obliged to refer to relevant GCs.[28] In October 2014, during the fourth plenary session of the Eighteenth Central Committee of the Communist Party of China, the Chinese leaders adopted the decision of the CPC Central Committee on "Several Major Issues Concerning the Comprehensive Promotion of the Rule of Law," setting forth, inter alia, the following goals: "strengthen and standardize [the systems] of judicial interpretations and case guidance, and unify the standards for the application of law."[29] Six months later, the Detailed Implementing Rules on the "Provisions of the Supreme People's Court Concerning Work on Case Guidance" was released by the SPC to provide judges with clearer guidance on how to cite GCs in similar subsequent cases.[30]

To date, the SPC has released eighty-seven GCs, covering a broad range of the legal field from criminal and administrative law through intellectual property and other areas of commercial law (such as contract, insurance, and company law) (see table 1).[31] Hundreds

Table 1: Number of GCs and Subsequent Cases Referencing GCs by Type

Type of Case	No. of GCs	No. of Subsequent Cases Referencing GCs (end of 2016)
Criminal	14	18
Administrative	14	92
Civil	54	409
– Tort	3	187
– Contract	12	146
– Company	2	22
– Enforcement	5	42
– Insurance	1	8
– Intellectual property and/or unfair competition	20	3
– Others (e.g., divorce)	11	1
Other (e.g., Maritime, State Compensation)	5	0
Total:	**87**	**519**

of subsequent cases from across China that reference these cases have been identified (181 and 519 by the end of 2015 and 2016, respectively) by the China Guiding Cases Project of Stanford Law School and posted online to facilitate legal research and practice.[32] Only three provinces or provincial-level regions—Gansu, Qinghai, and Tibet—have yet to produce judgments that are selected as GCs and have no cases referring to GCs (see table 2).[33] Within only six years, the Guiding Cases System has gained an impressive amount of momentum in a country that typically focuses on legislation only. The momentum is expected to grow because Judge Guo Feng, who oversees the selection of GCs, announced in his speech delivered to members of the American Chamber of Commerce in Beijing that the SPC plans to release an average of nearly one hundred GCs per year in the coming years.[34]

Of the eighty-seven GCs released thus far, none are related to cybersecurity, largely because the Cybersecurity Law of the People's Republic of China did not come into effect until June 2017.[35] However, and given widespread concerns about cybersecurity issues, including ICT-enabled theft of intellectual property,[36] it is encouraging to see that China has taken some steps, through the issuance of GCs related to the Internet, intellectual property, or both, to help improve the legal environment for the online protection of offline rights.

Guiding Case nos. 27, 29, and 45 are related to the Internet. Guiding Case no. 27 involves the commission of theft and fraud via the Internet; according to its Main Points of the Adjudication (a section in each GC summarizing its legal principles, which judges handling similar subsequent cases are expected to explicitly reference):[37]

> Where a perpetrator commits a crime by using an information network to trick another into clicking a false hyperlink and to actually steal property through a

Table 2: Number of GCs and Subsequent Cases Referencing GCs by Region

Province/ Provincial-Level Municipality	No. of GCs	No. of Subsequent Cases Referencing GCs (end of 2016)
Anhui	3	16
Beijing	5	17
Chongqing	1	13
Fujian	1	19
Gansu	0	0
Guangdong	1	70
Guangxi	0	4
Guizhou	1	7
Hainan	0	4
Hebei	0	18
Heilongjiang	1	7
Henan	1	42
Hubei	1	16
Hunan	0	9
Inner Mongolia	1	27
Jiangsu	14	43
Jiangxi	2	9
Jilin	0	9
Liaoning	0	14
Ningxia	0	2
Qinghai	0	0
Shaanxi	0	3
Shandong	4	76
Shanghai	11	15
Shanxi	0	1
Sichuan	5	12
Tianjin	3	9
Tibet	0	0
Xinjiang	0	3
Yunnan	0	1
Zhejiang	8	49
*Supreme People's Court	24	4
Total:	**87**	**519**

> computer program embedded in advance [in the hyperlink], [he][38] is to be convicted of and punished for theft. Where [a perpetrator] commits a crime by fabricating [the appearance of] tradable commodities or services and fraudulently acquiring property by deceiving another into clicking a payment hyperlink, [he] is to be convicted of and punished for fraud.

Guiding Case nos. 29 and 45 both invoke the Anti-Unfair Competition Law of the People's Republic of China in the context of the Internet.[39] The Main Points of the Adjudication of the former case are:

1. An abbreviated enterprise name that has been widely used externally by an enterprise for a long period of time, that has a certain degree of market visibility and is known to the relevant public, and that actually already functions as a trade name, may be regarded as an enterprise name and [thus] be protected [under law].

2. Where, without authorization, [a business operator] uses another's abbreviated enterprise name, which actually already functions as a trade name, as an Internet bid-for-ranking[40] keyword in business activities, causing the relevant public to be confused and to misidentify [the enterprise], [the unauthorized use of the abbreviated enterprise name] is an act of unfair competition.[41]

The Main Points of the Adjudication of Guiding Case no. 45 are:

> An act by [any] business operator engaged in Internet services that forcibly causes advertisements to pop up on the search results pages of other business operators' websites violates the principle of good faith and generally recognized business ethics, hinders the proper business operation of other business operators, and adversely affects their legal rights and interests. [Such an act] may, in accordance with the principles [set forth in] Article 2 of the *Anti-Unfair Competition Law of the People's Republic of China,* be determined to be unfair competition.[42]

As for intellectual property, there are already twenty IP-related GCs, half of which were released in March 2017. The SPC's growing interest in providing more guidance on intellectual property law via cases is also reflected in its support for the Beijing Intellectual Property Court, one of the three intellectual property courts in China, to develop a system of precedent-like cases and a clearer set of rules on how to apply these cases. This system will be formally launched later this year.[43] Experiences accumulated will help polish the system of GCs, especially those related to intellectual property.

There are no GCs on cybsersecurity issues, but such a GC is expected in the near future as critical ambiguities arising from the new Cybersecurity Law call for judicial clarifications. These ambiguities have caused Internet companies to express concerns about the protection of the rights of an individual, especially in combination with the onerous security requirements vaguely prescribed by the new law. For example, Article 28 provides:

> Network operators should provide technical support for and assistance in activities [carried out] in accordance with law by the public security organs and the state security organs to safeguard national security and investigate crimes.

Another example is Article 37, which states:

> Personal information and important data collected and generated by operators of critical information infrastructure during their operations within the territory of the People's Republic of China should be stored within the territory. Where, due to business needs, it is indeed necessary to provide [such information and data] to overseas [parties], a security assessment should be conducted in accordance with the measures formulated by the national cyberspace administration in conjunction with relevant departments of the State Council. Where laws and administrative regulations provide otherwise, their provisions shall be followed.

It is unclear how "operators of critical information infrastructure" (关键信息基础设施的运营者) are distinguished from regular "network operators" (网络运营者), except that Article 31(1) provides:

> For the critical information infrastructure in important industries and fields, including public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government affairs, and other [critical information infrastructure] that may seriously endanger national security, national economy and the people's livelihood, and public interest once it is damaged, loses functions, or has data leakage, the State shall, based on the hierarchical protection system for cybersecurity, implement key protection. The specific scope of critical information infrastructure and measures for their security protection shall be formulated by the State Council.

The concept of "critical information infrastructure" is not new. The US Critical Infrastructures Protection Act of 2001 defines the term "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[44] The US definition benefits from the country's system of precedents, which allows for judges to expound on the term in individual, concrete cases and thereby build on and refine it.[45] Likewise, it would be helpful if China could illustrate how the term "critical information infrastructure" is applied in practice, particularly in court. The author remains hopeful that the SPC can play an effective role in this respect, recalling the court's admirable efforts in helping to elaborate on the definition of the term "relevant market" appearing—but not clearly defined—in the Antimonopoly Law of the People's Republic of China.[46] As Judge John M. Walker, Jr., senior circuit judge of the US Court of Appeals for the Second Circuit, observed:[47]

> In Guiding Case No. 78, *Beijing Qihu Technology Co., Ltd. v. Tencent Technology (Shenzhen) Company Limited et al.*, the Chinese Supreme People's Court ("SPC") established authoritative guidance in the proper application of China's *Anti-Monopoly Law* to the

> evolving field of internet technology. The decision illuminates the SPC's carefully considered approach to questions of market definition and market dominance in the technology field. Jurists inside and outside China will find this approach useful.

In sum, if China continues using GCs to show how transparency and consistency can be achieved in the application of its Cybersecurity Law and related legal matters, such as intellectual property, China's pledge to equally protect the rights of individuals in both offline and online environments will be more warmly welcomed—as also the Code should be—by other countries, including the United States.

"Facilitate Access for All"

According to paragraph 2(8) of the Code, each state subscribing to the document pledges that "all States must play the same role in . . . international governance of the Internet . . . and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms" to, among other things, "facilitate access for all and ensure the stable and secure functioning of the Internet." China's pledge to "facilitate access for all" in cyberspace, in addition to advancing transparency and multilateral collaboration, presents business opportunities inside and outside the country. If these opportunities are made available to foreign businesses, the pledge may result in wider acceptance of the Code.

Outside China China's pledge to "facilitate access for all" in cyberspace is likely to create overseas business opportunities for Chinese companies, as reflected in the following paragraphs listed under the task titled "Digital Economy and Sharing of Digital Dividends" identified in the action plan of the Cyberspace Strategy 2017:[48]

> China supports assisting *developing countries* with cyber security capacity building, including technology transfer, critical information infrastructure development and personnel training, with a view to *turning the digital gap into digital opportunities so that more developing countries and their people will share the benefits of Internet development.*
>
> . . .
>
> China supports enhanced cooperation and sharing of Internet technology. It calls for countries to work together to address technological difficulties and *grow new industries and new business models through closer cooperation in network communication, mobile Internet, cloud computing, Internet of Things and big data.* Personnel exchange will be further enhanced to expand the rank of professionals strong in innovation.
>
> Keeping in mind the Belt and Road Initiative, China will encourage and support *Chinese Internet companies, together with those in the manufacturing, financial and ICT sectors,* to

> take the lead in going global, participate in international competition in line with the principle of fairness, explore international market and build cross-border industrial chain. *Chinese companies* will be encouraged to actively engage in capacity building of other countries and help *developing countries* with distance learning, remote health care and e-business among others to contribute to their social development (emphasis added).

It is not clear whether these business opportunities are available to both purely Chinese companies and foreign-invested enterprises (e.g., joint ventures and wholly foreign-owned enterprises), which, according to Chinese law, are also Chinese legal persons. It is even less clear whether foreign businesses that are not operating in China as foreign-invested enterprises can have a slice of this potentially big pie.

While it would be ideal for China to provide clarity, or at least some comments, on these issues, the United States need not and should not wait on the sidelines. Europe, admittedly encompassed physically in the Belt and Road Initiative in a way the United States cannot be, has been proactive in engaging with China at the intersection between business opportunities and international standard-setting (e.g., in connecting with Eurasia via trains, planes, and boats).[49] However, the United States could use its technological advantage to take the lead on virtual connectivity.

The United States has recently shown signs of interest in the Belt and Road Initiative. In particular, it reportedly supports China's Connectivity Plan.[50] The top Asia policy adviser to President Donald Trump has emphasized that "American companies will be able to provide the most valuable products and services" as they "have a long and proven track record in the global infrastructure market, and are ready to participate in Belt and Road projects."[51]

However, definite measures are still wanting. For example, some sources suggested that the United States, after attending the Belt and Road Forum for International Cooperation in Beijing on May 14–15 of this year, set up a working group to bring together authorities from Washington and Beijing along with stakeholders, including the private sector, to facilitate the involvement of US businesses in Belt and Road projects. However, no official announcement or major US news source has confirmed the establishment of such a working group.

It would be wise for the United States to interact with Chinese authorities in order to identify business opportunities, in particular for American businesses, along the Belt and Road route. In this way, the United States may weigh the advantages and disadvantages of paragraph 2(8) and the Code more broadly.

Inside China China, as discussed above, perceives a need to "tur[n] the digital gap into digital opportunities so that more developing countries and their people will share the benefits of Internet development." In fact, this need should apply to not only developing

countries but also less-developed regions within China, where the digital gap—partly due to inadequate telecommunications infrastructure—has limited many Chinese people's access to the Internet.[52] Will China's pledge in the Code to "facilitate access for all" in cyberspace create business opportunities within the country for foreign companies, in the same or a similar manner, mentioned above, as overseas business opportunities are created for Chinese companies? The answer to this question involves two other, more specific, inquiries. First, considering the authorities' control over the Internet, is China ready to "facilitate access for all" in its own territory? Second, even if China is ready, wouldn't purely Chinese companies be favored, as investment in this area may be considered rather sensitive? The following paragraphs discuss these two inquiries in turn.

Contrary to conventional wisdom, China began its "openness" journey at the turn of the twenty-first century, when Chinese scholars were discussing the concept of "reinventing government" or "reengineering government" as the new approach to public administration. The discussions, together with the government reforms implemented in China at the time, culminated in the emergence of a belief that the ultimate goal of various administrative reforms was to have "open government" (开放政府) featuring openness and transparency, citizen participation, and government integrity. Since the release of the Open Government Directive by the Obama administration in 2009, many scholars in China have discussed the principles of transparency, participation, and collaboration stated in the directive and their potential impact in China. They generally acknowledge that, in China, the establishment of open government is a natural step following the development of the e-government initiative that started in 2001, when the National Informatization Leading Group was formed.[53]

The milestones of China's e-government initiative have been marked by the release of a series of important documents, including (1) the National Informatization Development Strategy (2006–2020), which listed e-government as a strategic priority for encouraging administrative efficiency, government efficacy, and democratic participation; (2) the Overall Framework for National E-Government Affairs (2006), which urged the enactment of government information disclosure legislation; (3) the Regulation of the People's Republic of China on Open Government Information (2007), which was promulgated by the State Council to set a national standard for open government information; and (4) the Twelfth Five-Year Plan of National E-Government Affairs (2011–15), which redefined e-government as a "strategic initiative to deepen the reforms in the administrative system and build a service-oriented government with which the citizens are satisfied" and which emphasized citizens' right to know and right to participate.[54]

The year 2014 saw two important developments in China's "openness" journey. First, the term "open government" (开放政府) was used for the first time in an official document: the Notice Concerning Speeding Up the Implementation of Work Related to the Information-for-Citizens Project (2014), which was jointly issued by a dozen ministries and important leaders' groups, including the National Development and Reform Commission, the

Ministry of Industry and Information Technology, the Ministry of Finance, the Ministry of Education, the Ministry of Public Security, the Ministry of Civil Affairs, and the Ministry of Human Resources and Social Security. The notice identified various priorities, including the development of open government data and open government by building systems needed for disclosing and sharing government data, treating government data resources as public resources, and promoting the transparency of the government and the interaction between the government and citizens.[55]

Second, Guiding Case no. 26,[56] which applies the Regulation on Open Government Information, was released. The Main Points of the Adjudication section of the case reads:

> Where a citizen or a legal person or other organization submits an application for the disclosure of government information to an administrative organ through a governmental public network system, if the network system does not state otherwise, the date on which the system confirms the successful submission of the application should be regarded as the date on which the administrative organ receives the application for the disclosure of government information. The administrative organ's internal processing procedure for the application cannot be a ground for [justifying] the administrative organ's deferred processing [of the application]. [The resulting] delay in issuing a reply should be recognized as a violation of law.

The recent release, for comment, of a draft amendment to the Regulation on Open Government Information seems to suggest that the Chinese authorities are ready to take another step in the promotion of the openness culture in China. Among various proposed revisions, the draft amendment includes the principle of "making [government information] open as the norm and not making it open as an exception" (以公开为常态、不公开为例外).[57] This development renders China's pledge in the Code to "facilitate access for all" within its own territory more convincing.

But will China grant foreign investors related business opportunities to make this pledge truly appealing to Western countries, such as the United States? In October 2016, China ushered in a novel foreign investment regime by promulgating a new basic regulation governing registration of foreign-invested enterprises[58] and by making corresponding changes to legislation concerning joint ventures and wholly foreign-owned enterprises. The essence of the new regime is to change the regulation of foreign-invested enterprises from a system that requires approval from the Ministry of Commerce to a simple registration system. Foreign-invested enterprises that are not restricted under the so-called National Negative List can now complete their formation and make most structural changes by simply following an online registration process. The purpose of this new regime is, according to China, to "further expand [the country's] opening up, promote the reform of the foreign investment administration system, and create a rule-of-law, international, and convenient business environment."[59]

Given this purpose, many foreign investors hoped that the National Negative List would be rather simple and short. Unfortunately, it is now clear that the Catalogue of Industries for Guiding Foreign Investment (revised in 2015), which is complicated and includes a lengthy enumeration of industries in which foreign investment is prohibited or restricted, is being used as the National Negative List. It will be helpful if China clearly explains how foreign companies can rely on China's pledge to "facilitate access for all" in cyberspace to tap into the Chinese market. For example, the Cybersecurity Law only came into effect recently. One would like to know what opportunities or impediments foreign companies can expect in the ICT space given that the Cybersecurity Law places a lot of weight on several aspects of critical information infrastructure and yet this term is defined only vaguely in this new law and not at all in the Catalogue.

Suggestions for the United States and China

In heated debates among stakeholders who strive to advance their interests—be they political, ideological, economic, or of another kind—through the development of cybernorms, stakeholders often forget that the process is dynamic and evolving. In their article titled "Constructing Norms for Global Cybersecurity," Finnemore and Hollis emphasize what others often forget:[60]

> The success of a norm rests not just in what it says, but in who accepts it. . . . It matters to the content and future of a norm, for example, whether it is promulgated by states at the United Nations, technologists in an industry association, privacy activists in a nongovernmental organization (NGO), or some freestanding multistakeholder group open to all these actors. . . . Norms have an inherently dynamic character; they continuously develop via ongoing processes in which actors extend or amend their meaning as circumstances evolve. This suppleness is part of their attraction, but managing this dynamism also requires foresight currently lacking among those seeking to construct cybernorms.

Identifying cybernorms that are acceptable to the United States and China is thus understandably difficult. However, recent developments in China, as discussed above, show that paragraphs 2(7) and 2(8) of the Code present opportunities for the two countries to reach some consensus on setting appropriate norms of state behavior in cyberspace. To seize these opportunities, the United States and China should develop deep and practical confidence-building measures to pave the way for success. This step is in line with both the Code and the Cybersecurity Law and should, therefore, be welcomed by China. Paragraph 2(10) of the Code requires each state subscribing to the document:

> To develop *confidence-building measures aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict.* Such measures will include, *inter alia,* voluntary exchange of information regarding national strategies and

> organizational structures for ensuring a State's information security, the publication of white papers and exchanges of best practice [sic], wherever practical and advisable (emphasis added).

Article 7 of the Cybersecurity Law charges China to "actively carry out international exchange and cooperation in terms of cyberspace governance, research and development of network technologies, formulation of standards thereof," and so on, so as to "establish a multilateral, democratic and transparent system for cyber governance."

These confidence-building measures could be developed via the ongoing meetings of the US-China senior experts group set up to discuss appropriate norms of state behavior in cyberspace. In addition, they could be developed via the US-China Comprehensive Dialogue that the two countries have established since President Trump met with President Xi at the Mar-a-Lago resort in Florida earlier this year.[61] The Dialogue is reportedly overseen by the two presidents and has four dimensions: the diplomatic and security dialogue, the comprehensive economic dialogue, the law enforcement and cybersecurity dialogue, and the social and cultural issues dialogue.

In particular, based on the above analysis, the two sides should exchange up-to-date information about (1) how significant cases, for example, GCs and other special cases in China, together with similar subsequent cases, as well as Supreme Court cases in the United States, have been used to help improve the legal environment for the protection of rights associated with the Internet; and (2) what business opportunities inside and outside China are available to foreign companies in connection with China's objective to "facilitate access for all" in cyberspace. With respect to GCs and other court cases referred to in the first point, it should be noted that judicial reform in China has already become an important topic for discussion in US-China relations. According to the Outcome List of President Xi Jinping's State Visit to the United States, the two countries reached consensus on, among others, the following:

> China and the United States commit to conduct high-level and expert discussions commencing in early 2016 to provide a forum to *support and exchange views on judicial reform and identify and evaluate the challenges and strategies in implementing the rule of law.* U.S. participants are to include leading members of the U.S. judiciary, U.S. government legal policy experts, and officials from the Departments of Commerce and Justice and the Office of the United States Trade Representative. Chinese participants are to include officials from the Central Leading Group on Judicial Reform, leading members of the Chinese judiciary, and Chinese government legal policy experts. *This dialogue is to result in an improvement in the transparency and predictability of the business environment.* This dialogue does not replace, duplicate or weaken existing regular bilateral legal and human rights dialogues between China and the United States. (emphasis added).[62]

The two sides held the first dialogue of this type in early August 2016 to discuss, among other issues, "efficiency and fairness in handling commercial cases and the use of Guiding Cases in the adjudication of commercial [cases]."[63] The second dialogue of this type has been scheduled for 2017.[64]

Bearing in mind Finnemore and Hollis's observation that "the success of a norm rests not just in what it says, but in who accepts it," China and the United States should recognize that the Code—any code produced solely by governments—will lack the rigor to serve as anything other than a high-level framework. In the effort to formulate and implement a code that will "establish an information environment that is peaceful, secure, open," governments should cooperate not only among themselves but also with the businesses that develop, support, and know cyberspace as well as, if not better than, governments. Indeed, governments repeatedly and publicly agree to do so (e.g., in the G20 Digital Economy Development and Cooperation Initiative, which came out of the 2016 G20 Leader's Summit held in Hangzhou, China).[65]

Instead of each government and each tech giant proposing norms anew and at odds with one another, each actor should use its leverage to engage with and help develop existing initiatives, the fewer the better. This author proposes that all actors, from China, the United States, and the United Nations, to IT companies such as Microsoft and Alibaba, focus on the Code for the following reasons:

- The Code has already garnered significant international support. It can count on support from the six states of the SCO which submitted it and probably any states that hereafter join the SCO (such as Pakistan and India, which just joined) as well as at least some of the nearly one hundred states of the Belt and Road Initiative. The European Parliament is working to "clarify the positions promoted" in the Code.[66]

- The Code is relatively simple and unencumbered by specifics. There is a lot of leeway for other stakeholders to help shape the Code and develop its details and the specific measures for implementing it.

- The Code is a rather rare instance of China taking an active role in setting international standards that potentially impose onerous responsibilities on itself and its allies. If other actors engage with China via the Code, China might reciprocate by stepping up its own engagement to build its reputation as a global leader, leading to effective and enforced international norms in cyberspace and, likely, goodwill and an example for engagement in other areas of international cooperation.

The United States and China have many different views about cyberspace. Clearly, the two countries' cyber relations must be considered with a broader context in mind, including

the overall strategic roles that each country plans to play in an increasingly complex world. Whatever competing interests they may have, the ultimate goal should be conducive to building sustainable peace for all. Finding common ground between these two global powers is an arduous but necessary task.

NOTES

1 White House, Office of the Press Secretary, "President Xi Jinping's State Visit to the United States," news release, September 25, 2015, accessed July 18, 2017, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. See also, Ministry of Foreign Affairs of the People's Republic of China, "Full Text: Outcome List of President Xi Jinping's State Visit to the United States," September 26, 2015, accessed July 18, 2017, www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1300771.shtml.

2 See Hua Xia, "China, U.S. Discuss Int'l Norms of State Behavior in Cyber Space," *Xinhua,* May 12, 2016, accessed July 18, 2017, http://news.xinhuanet.com/english/2016-05/12/c_135354264.htm.

3 International Code of Conduct for Information Security, transmitted by "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," UN Doc. A/69/723, January 13, 2015, accessed July 18, 2017, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

4 Ibid.

5 "Statement by Ms. Lyu Xin of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 71st Session of the UN General Assembly," Permanent Mission of the People's Republic of China to the UN, October 24, 2016, accessed July 18, 2017, www.china-un.org/eng/hyyfy/t1408980.htm.

6《网络空间国际合作战略》(Preface, "International Strategy of Cooperation on Cyberspace"), issued by the Ministry of Foreign Affairs of the People's Republic of China on March 1, 2017, accessed July 18, 2017, www.scio.gov.cn/32618/Document/1543874/1543874.htm.

7 Ibid., chapter 2, Basic Principles (including four sections: 1. The Principle of Peace; 2. The Principle of Sovereignty; 3. The Principle of Shared Governance; and 4. The Principle of Shared Benefits).

8 Ibid., chapter 3, Strategic Goals (including six sections: 1. Safeguarding Sovereignty and Security; 2. Developing A System of International Rules; 3. Promoting Fair Internet Governance; 4. Protecting Legitimate Rights and Interests of Citizens; 5. Promoting Cooperation on Digital Economy; and 6. Building Platform for Cyber Culture Exchange).

9 Ibid., chapter 4, Plan of Action (including nine sections: 1. Peace and Stability in Cyberspace; 2. Rule-based Order in Cyberspace; 3. Partnership in Cyberspace; 4. Reform of Global Internet Governance System; 5. International Cooperation on Cyber Terrorism and Cyber Crimes; 6. Protection of Citizens' Rights and Interests Including Privacy; 7. Digital Economy and Sharing of Digital Dividends; 8. Global Information Infrastructure Development and Protection; and 9. Exchange of Cyber Cultures).

10 Ibid., chapter 4, Plan of Action, Section 2 (Rule-based Order in Cyberspace).

11 "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 26, 2015, UN Doc. A/70/174, accessed July 18, 2017, www.un.org/Docs/journal/asp/ws.asp?m=A/70/174.

12 See, e.g., Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity," *The Diplomat,* January 19, 2017, accessed July 18, 2017, http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity.

13 See, e.g., Sarah McKune, "Will the SCO States' Efforts to Address 'Territorial Disputes' in Cyberspace Determine the Future of International Human Rights Law?" *The Citizen Lab,* September 28, 2015, accessed July 18, 2017, https://citizenlab.org/2015/09/international-code-of-conduct.

14 Charter of the Shanghai Cooperation Organization, Article 1, accessed July 18, 2017, en.sco-russia.ru/load/1013181846.

15 Stephen Aris, "The Shanghai Cooperation Organisation: 'Tackling the Three Evils.' A Regional Response to Non-Traditional Security Challenges or an Anti-Western Bloc?" *Europe-Asia Studies* 61, no. 3 (May 2009): 457, accessed July 18, 2017, https://www.jstor.org/stable/27752254?seq=1#page_scan_tab_contents.

16 "General Information," The Shanghai Cooperation Organization, accessed July 18, 2017, http://eng.sectsco.org/cooperation.

17 See Ministry of Foreign Affairs of the People's Republic of China, "Shanghai Cooperation Organization," January 7, 2004, accessed July 18, 2017,www.fmprc.gov.cn/mfa_eng/topics_665678/sco_665908/t57970.shtml.

18 UN Refugee Agency, "Shanghai Convention on Combating Terrorism, Separatism and Extremism," accessed July 18, 2017, www.refworld.org/docid/49f5d9f92.html.

19 "China Focus: SCO Expansion Vital for Int'l Security, Common Prosperity," *Xinhua,* June 10, 2017, accessed July 18, 2017, http://news.xinhuanet.com/english/2017-06/10/c_136355540.htm.

20 "About SCO," The Shanghai Cooperation Organization, accessed July 18, 2017, http://eng.sectsco.org/about_sco.

21 Data compiled by the China Guiding Cases Project (CGCP) with reference to its list of Belt and Road countries, accessed July 18, 2017, https://cgc.law.stanford.edu/belt-and-road/b-and-r-countries.

22 Ministry of Foreign Affairs of the People's Republic of China, "Shanghai Cooperation Organization."

23 "Urgent: China Takes over Rotating Chair of SCO," *Xinhua,* June 9, 2017, accessed July 18, 2017, http://news.xinhuanet.com/english/2017-06/09/c_136353362.htm.

24 "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/68/98, paragraph 19, June 24, 2013, accessed July 18, 2017, https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf; see also "Resolution adopted by the General Assembly on 23 December 2015," ("welcoming" the aforementioned conclusion in the UNGGE's 2013 report), accessed July 18, 2017, https://ccdcoe.org/sites/default/files/documents/UN-151223-ITIS.pdf.

25 For more discussion of this observation, see Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *Citizen Lab,* accessed July 18, 2017, https://openeffect.ca/code-conduct.

26 UN General Assembly, "The Right to Privacy in the Digital Age," December 18, 2013, 2, accessed July 18, 2017, www.un.org/Docs/journal/asp/ws.asp?m=A/RES/68/167.

27 《最高人民法院关于案例指导工作的规定》("Provisions of the Supreme People's Court Concerning Work on Case Guidance"), passed by the Adjudication Committee of the Supreme People's Court on November 15, 2010, issued on and effective as of November 26, 2010, Stanford Law School China Guiding Cases Project, English Guiding Cases Rules, June 12, 2015, edition, accessed July 18, 2017, http://cgc.law.stanford.edu/guiding-cases-rules/20101126-english. See also 郭锋法官 (Judge Guo Feng), 中国法院指导性案例的编选与适用 ("The Compilation and Application of China's Guiding Cases"), 斯坦福法学院中国指导性案例项目, Stanford Law School China Guiding Cases Project, January 27, 2017, accessed July 18, 2017, http://cgc.law.stanford.edu/commentaries/18-guo-feng.

28 《最高人民法院关于案例指导工作的规定》("Provisions of the Supreme People's Court Concerning Work on Case Guidance"), Article 2, which provides:

> The Guiding Cases referred to in this [set of] Provisions [must be] rulings and judgments that have already come into legal effect and meet the following requirements:
>
> (1) are of widespread concern to society;
> (2) [involve] legal provisions [that] are of relatively general nature;
> (3) are of a typical nature;
> (4) are difficult, complicated, or of new types; [or]
> (5) other cases which have guiding effect.

29 《中共中央关于全面推进依法治国若干重大问题的决定》("Decision of the CPC Central Committee on Several Major Issues Concerning the Comprehensive Promotion of the Rule of Law"), passed at the fourth plenary session of the Eighteenth Central Committee of the Communist Party of China on October 23, 2014, accessed July 18, 2017, www.gov.cn/xinwen/2014-10/28/content_2771714.htm.

30 《〈最高人民法院关于案例指导工作的规定〉实施细则》("Detailed Implementing Rules on the 'Provisions of the Supreme People's Court Concerning Work on Case Guidance"), passed by the Adjudication Committee of the Supreme People's Court on April 27, 2015, issued on and effective as of May 13, 2015, Stanford Law School China Guiding Cases Project, English Guiding Cases Rules, June 12, 2015 edition, http://cgc.law.stanford.edu/guiding-cases-rules/20150513-english.

31 See Mei Gechlik, "China's Guiding Cases System: Review and Recommendations," Stanford Law School China Guiding Cases Project, Guiding Cases Analytics, no. 6, August 2017 (forthcoming).

32 Full text judgments and rulings referencing GCs can be found at https://cgc.law.stanford.edu/judgments; for an analysis of these and similar subsequent cases, see Mei Gechlik and Minmin Zhang, "Cumulative Analysis of All Subsequent Cases Referring to Guiding Cases in China (2014 Q1-2016 Q4)," Stanford Law School China Guiding Cases Project, Guiding Cases Surveys, no. 3, August 2017 (forthcoming).

33 Gechlik and Zhang, "Cumulative Analysis."

34 Judge Guo Feng and the author spoke on "Guiding Cases and Their Importance to China's Belt and Road Initiative" at the American Chamber of Commerce in Beijing, June 16, 2017.

35 《中华人民共和国网络安全法》("Cybersecurity Law of the People's Republic of China"), passed and issued on November 7, 2016, effective as of June 1, 2017.

36 At the Antalya summit in 2015, the G20 countries released a communiqué "affirm[ing] that no country should conduct or support ICT-enabled theft of intellectual property," November 15–16, 2015, accessed July 18, 2017, http://g20.org.tr/g20-leaders-commenced-the-antalya-summit. At the 2016 G20 summit, which was hosted by China in Hangzhou, Zhejiang Province, the communiqué included a specific "reaffirm[ation]" of this paragraph of the Antalya Communiqué. See G20 Leaders' Communiqué, Hangzhou Summit, September 4–5, 2016, accessed July 18, 2017, www.g20chn.org/English/Documents/Current/201609/t20160906_3395.html. In addition, the Leaders' Declaration from the 2016 APEC Economic Leaders' Meeting (the United States and China are members, among about twenty others) includes a similar reference to ICT-enabled theft of intellectual property: "We also affirm that economies should not conduct or support ICT-enabled theft of intellectual property or other confidential business information, with the intent of providing competitive advantages to companies and commercial sectors." See 2016 Leaders' Declaration, 2016 APEC Economic Leaders' Meeting, November 20, 2016, accessed July 18, 2017, www.apec.org/Meeting-Papers/Leaders-Declarations/2016/2016_aelm.aspx.

37 《臧进泉等盗窃、诈骗案》("Zang Jinquan et al., A Theft and Fraud Case"), Stanford Law School China Guiding Cases Project, English Guiding Case (EGC27), October 20, 2014, edition, accessed July 18, 2017, http://cgc.law.stanford.edu/guiding-cases/guiding-case-27.

38 "He" as used in this quotation is a gender-neutral term that may refer to "she" and "it."

39《中华人民共和国反不正当竞争法》(“Anti-Unfair Competition Law of the People’s Republic of China”), passed and issued on September 2, 1993, effective as of December 1, 1993, accessed July 18, 2017, www.npc.gov.cn/wxzl/wxzl/2000-12/05/content_4600.htm.

40 “Internet bid-for-ranking” (竞价排名) is a means of bidding for a higher position on an online search results page. For more information on the topic, see http://baike.baidu.com/view/40571.htm (accessed July 18, 2017).

41《天津中国青年旅行社诉天津国青国际旅行社擅自使用他人企业名称纠纷案》(“Tianjin China Youth Travel Service v. Tianjin Guoqing International Travel Agency, A Dispute over an Unauthorized Use of Another’s Enterprise Name”), Stanford Law School China Guiding Cases Project, English Guiding Case (EGC29), October 20, 2014, edition, accessed July 18, 2017, http://cgc.law.stanford.edu/guiding-cases/guiding-case-29.

42《北京百度网讯科技有限公司诉青岛奥商网络技术有限公司等不正当竞争纠纷案》(“Beijing Baidu Netcom Science and Technology Co., Ltd. v. Qingdao Aoshang Network Technology Co., Ltd., An Unfair Competition Dispute”), Stanford Law School China Guiding Cases Project, English Guiding Case (EGC45), November 15, 2015, edition, accessed July 18, 2017, http://cgc.law.stanford.edu/guiding-cases/guiding-case-45.

43 The author met with the company developing this database for the Beijing IP Court in June 2017.

44 42 U.S. Code § 5195c(e).

45 See, e.g., In Re State, 325 S.W.3d 848 (Tex. Ct. App. 2010).

46《中华人民共和国反垄断法》(“Anti-Monopoly Law of the People’s Republic of China”), passed and issued on August 30, 2007, effective as of August 1, 2008, accessed July 18, 2017, www.gov.cn/flfg/2007-08/30/content_732591.htm.

47 John M. Walker Jr., “In Qihu v. Tencent, the Chinese Supreme People’s Court Offers Antitrust Insight for the Digital Age,” Stanford Law School China Guiding Cases Project, China Cases Insights, no. 1, May 5, 2017, accessed July 18, 2017, http://cgc.law.stanford.edu/commentaries/1-insights-2017-john-walker.

48《网络空间国际合作战略》(“International Strategy of Cooperation on Cyberspace”), IV.7.

49 See, e.g., Jan Gaspers, “Germany Wants Europe to Help Shape China’s Belt and Road Initiative,” *The Diplomat,* December 17, 2017, accessed July 18, 2017, http://thediplomat.com/2016/12/germany-wants-europe-to-help-shape-chinas-belt-and-road-initiative; see also “Frequently Asked Questions on EU–China Relations,” European Commission, June 1, 2017, accessed July 18, 2017, http://europa.eu/rapid/press-release_MEMO-16-2258_en.htm.

50 See Sue-Lin Wong, “United States Says It Supports China’s Infrastructure Connectivity Plan,” *Reuters,* May 14, 2017, accessed July 18, 2017, www.reuters.com/article/us-china-silkroad-usa-idUSKCN18A0D2.

51 See “US Belt and Road Working Group Is Sign of Increased Interest in Cooperation with China, says WSJ,” *Medium,* May 15, 2017, accessed July 18, 2017, https://medium.com/@yicaichina/us-belt-and-road-working-group-is-sign-of-increased-interest-in-cooperation-with-china-says-wsj-c1b2a0b2174b.

52 Mei Gechlik et al., “The China eGovernment Development Index Report 2013: Experiences in Hangzhou Municipality, Zhejiang Province,” *Good Governance International,* 2013.

53 Mei Gechlik, Dai Di, and Jordan Corrente Beck, “Open Judiciary in a Closed Society: A Paradox in China?” in *Achieving Open Justice through Citizen Participation and Transparency,* eds. Carlos E. Jiménez-Gómez and Mila Gascó-Hernández (Hershey, PA: IGI Global, 2016).

54 Ibid.

55 Ibid.

56《李健雄诉广东省交通运输厅政府信息公开案》(“LI Jianxiong v. Department of Transport of Guangdong Province, A Case About Open Government Information”), Stanford Law School China Guiding Cases Project, English Guiding Case (EGC26), April 4, 2014, edition, accessed July 18, 2017, http://cgc.law.stanford.edu/guiding-cases/guiding-case-26.

57 政府信息公开条例首次修订 (“First Amendment to the Regulation on Open Government Information”),《人民日报》(*People’s Daily*), June 7, 2017, accessed July 18, 2017, http://paper.people.com.cn/rmrb/html/2017-06/07/nw.D110000renmrb_20170607_1-13.htm.

58《外商投资企业设立及变更备案管理暂行办法》(“Interim Measures for the Recordation Administration of the Formation and Modification of Foreign-Invested Enterprises”), passed by the Ministry of Commerce of the People’s Republic of China on and effective as of October 8, 2016.

59 Ibid., Article 1.

60 Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal Of International Law* 110, no. 3 (July 2016): 425.

61 “Trump, Xi Establish US-China Comprehensive Dialogue,” *The Tribune,* April 8, 2017, accessed July 18, 2017, www.tribuneindia.com/news/world/trump-xi-establish-us-china-comprehensive-dialogue/388938.html.

62 Ministry of Foreign Affairs of the People’s Republic of China, “Outcome List of President Xi Jinping’s State Visit to the United States.”

63 李阳 (Li Yang), 中美举行首次法治对话 第二次将在华盛顿举行 (“China and the United States Had the First Dialogue on the Rule of Law; The Second One Will Be Held in Washington”),《人民法院报》(*People’s Court Daily*), August 5, 2016, accessed July 18, 2017, www.chinacourt.org/article/detail/2016/08/id/2051182.shtml.

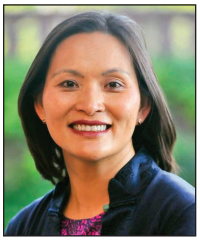
64 Ibid.

65 G20 Digital Economy Development and Cooperation Initiative, Hangzhou Summit, September 4–5, 2016, accessed July 18, 2017, www.g20chn.org/English/Documents/Current/201609/P020160908736971932404.pdf.

66 European Parliament Research Service, October 2015 Briefing, “Cyber Diplomacy: Confidence-building Measures,” 11, accessed July 18, 2017, www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS BRI(2015)571302_EN.pdf.

The preferred citation for this publication: Mei Gechlik, **Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses**, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1706 (July 28, 2017), available at https://lawfareblog.com/appropriate-norms-state-behavior-cyberspace-governance-china-and-opportunitites-us-businesses.

About the Author



MEI GECHLIK

Mei Gechlik is founder and director of the China Guiding Cases Project (CGCP) at Stanford Law School. Formerly a tenured professor in Hong Kong, she founded the CGCP in February 2011. With support from an international team of nearly two hundred members and an advisory board of approximately fifty distinguished experts, including justices from the US Supreme Court and China's Supreme People's Court, the CGCP has quickly become the premier source of analyses of Guiding Cases, China's de facto binding case law (http://cgc.law.stanford.edu). The CGCP has presented at several notable forums, including the World Bank, the Open Government Partnership Global Summit, and a US-China Legal Exchange Conference. From 2001 to 2005, Gechlik worked for the Carnegie Endowment for International Peace, a Washington, DC-based think tank, testifying before the US Congress on various topics about China. Gechlik is admitted as a barrister in England, Wales, and Hong Kong and is a member of the bar in New York and the District of Columbia. She received her doctorate in the science of law from Stanford Law School and her MBA in finance from the Wharton School at the University of Pennsylvania.

Synopsis

Finding cybernorms that are acceptable to the United States and China, which have different ideologies and practices as well as enormous interests at stake, is challenging. However, recent developments in China show that the International Code of Conduct for Information Security that China and other member states of the Shanghai Cooperation Organization submitted to the General Assembly of the United Nations in 2015, especially paragraphs 2(7) (protecting online and offline rights equally) and 2(8) (facilitating access for all in cyberspace), present new opportunities for the two countries to bridge certain gaps in setting cybernorms. This essay identifies these developments in China—the new Guiding Cases System as well as foreign and domestic developments regarding facilitating everyone's access to cyberspace—and discusses how they, together with the Shanghai Cooperation Organization's growing significance in the international arena, call for more strategic thinking among US policymakers so that the United States can seize the new opportunities to engage meaningfully with China in establishing international norms for cyberspace.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION