Global Cyber Governance

China's Contribution and Approach

Cai Cuihong

Abstract: With the world's largest number of netizens, China has been engaged in the ever more intense global competition for cyber governance over the past decade. Based on some preliminary studies, this article discusses China's position, approach and contribution to global cyber governance, as well as the understanding gap on major issues between China and developed countries in the cyber arena. In the past decade, China has made significant contributions to the reform of global cyber governance utilizing a "patch-work" approach, and it will try to play a more active role as a constructive participant in global cyber governance while enhancing its own cyber capacity. Unlike many developed countries that advocate "Internet freedom," China will continue to uphold the principle of cyber sovereignty. Yet in the meantime, China will try to work with other countries to build a "Community of Shared Future in

Cai Cuihong is Professor at the Center for American Studies, Fudan University. Her mailing address is: Center for American Studies, Fudan University, 220 Handan Road, Shanghai 200433, China. She can also be reached at chcai@fudan.edu.cn.

© 2018 World Century Publishing Corporation and Shanghai Institutes for International Studies
China Quarterly of International Strategic Studies, Vol. 4, No. 1, 55–76
DOI: [10.1142/S2377740018500069](https://doi.org/10.1142/S2377740018500069)

This is an Open Access article, copyright owned by the SIIS and WCPC. The article is distributed under the Creative Commons Attribution 4.0 (CC BY-NC) Licence. Further distribution of this work is permitted, provided the original work is properly cited and for non-commercial purposes.

Cyberspace,” in order to promote freedom, democracy and transparency in cyberspace in an incremental, stable and reasonable way.

Keywords: Global governance; multilateralism; multi-stakeholder; cyber sovereignty; “Community of Shared Future in Cyberspace.”

As an emerging topic in global governance, global cyber governance deals not only with cyber infrastructure, coding and specification, but also cyber security and other economic and cultural issues related to the Internet. In general, there exist two major approaches in the current landscape of global cyber governance. One is the technical approach, which can be described as a fusion of the market and society, and also a spontaneous arrangement based on rough consensus. From a technical point of view, the Internet is still a continuation of the experimental ARPANET created by the U.S. Defense Advanced Research Projects Agency more than 30 years ago.¹ The other is the regulatory approach which is centered on sovereign governments, such as the control of cyber activities by domestic law and the relative discourse power of countries in global governance.

Due to their differences in cyber capacity, power status, law, and culture, countries of the world find themselves in lasting disputes over such issues as whether to maintain or reform the current global cyber governance structure, whether to follow a multi-stakeholder model or a multilateral model, and whether to set up some new institutions for cyberspace or incorporate the cyber issue into existing institutions, to name just a few.² In short, cyber governance is the focus of intensifying global debate.

In a similar vein, the research literature in English on China's participation in global cyber governance also follows two trends in general. One initiates discussion on the role of non-state actors in the overall policy process, and the other explores some specific problems regarding China's participation in global cyber governance.³ This article aims to analyze

¹NCAFP, “Cyberpower and National Security,” *American Foreign Policy Interests*, Vol. 35, No. 1 (2013), p. 48.

²Cai Cuihong, “The Cyberspace Governance amid the Interaction of States, Markets and Society,” *World Economics and Politics*, No. 9 (2013), pp. 101–103.

³Tristan Galloway and He Baogang, “China and the Global Internet Technological Governance” (translated by Wang Min), *Journal of Cyber Affairs*, No. 6 (2016), pp. 80–91.

China's overall position and views on global cyber governance, as well as the understanding gap between China and developed countries in the cyber arena, in order to resolve some of misunderstandings that are fueling the international disputes on global cyber governance.

This article is divided into three sections. The first examines China's role and contributions in maintaining a safe, free and stable cyberspace; the second discusses China's position and approach to global cyber governance; and the third analyzes the consensus and differences between China and developed countries in the basic principles, norms, rules and architecture of global cyber governance. It concludes that in the future, China is expected to play a more active and important role in global cyber governance as a constructive and responsible participant.

China's Contribution to Global Cyber Governance

China has the world's largest number of Internet users. As its dependence on the Internet continues to grow, China has been engaged in the ever more intense global competition for cyber governance over the past decade. In retrospect, China's active participation in global cyber governance began with Edward Snowden's revelations of the Prism Scandal, which made the Chinese government fully aware of the threats from the cyber world and the absolute necessity for it to work with the international community to maintain a safe, free and stable cyberspace. Yet China's proactive participation and its position on global cyber governance, in particular its proposal of "cyber sovereignty," have triggered much debate in the West. China's actions in cyberspace, including its sponsorship of the World Internet Conference, are perceived by developed countries as a window to observe the Chinese government's position on internet freedom.⁴ And many see China striving for leadership in the global governance of cyberspace.⁵

⁴Franz-Stefan Gady, "The Wuzhen Summit and the Battle over Internet Governance," *Diplomat*, January 14, 2016, <https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-Internet-governance/>.

⁵"China Seeks World Leadership Role in Internet Governance," Associated Press, March 5, 2017, <https://businessmirror.com.ph/china-seeks-world-leadership-role-in-Internet-governance/>.

With growing power and interest in cyberspace, China has felt it imperative to take an active part in global cyber governance. China's participation not only helps promote its own interest in cyberspace, but also generates international implications with regard to the major trends of global cyber governance, including, for example, the democratization of international relations, the relative statuses of different actors involved, transition of cyberspace problems, and the coordination of values for global cyber governance.

Above all, China's participation in global cyber governance contributes to democratization of international relations and the evolution of the international system. This is because China's extensive engagement is not only conducive to its own development, but also provides momentum for maintaining the cyberspace order and fostering fairer and more just international relations. The essence of democratization of international relations is that all countries have the right to make decisions for themselves; disputes must be settled through consultation and negotiation by concerned parties on equal footing; and global challenges should be dealt with through cooperation among all countries.⁶ Thus, China has been advocating that all central governments should be equally involved in the formulation of common rules for cyberspace, in order to safeguard the sovereignty and national interest of itself and other developing countries.

China actively participates in global cyber governance to safeguard its cyber sovereignty and national interest.

In fact, the dispute over China's position in global cyber governance is not between China and the rest of the world, but between Western powers and the vast developing world instead. With their dominant position in the current global governance system, developed countries have largely written international rules and norms on cyberspace to reflect their own values and meet their own interests. However, with the "southward" development of the Internet, Internet users from developing countries have now exceeded 50 percent of the world's total. According to estimates by the Microsoft Corporation, there will be 4.7 billion Internet users around the world by

⁶Jiang Zemin, *Selected Works of Jiang Zemin* (Vol. 3) (Beijing: Remin Press, 2006), p. 474.

2025, of which 75 percent will be from emerging economies.⁷ Therefore, in order to gain a role proportionate to their rising power, the interest and demand of developing countries in global cyber governance is greatly needed.

Next, China's engagement in global cyber governance promotes the evolution of the statuses and roles of different actors in cyberspace. Both the multilateralism and multi-stakeholder approaches recognize the role of different actors in global cyber governance; their major difference lies in the positioning of those actors, particularly in who is to play a dominant role. Indeed, in global cyber governance, the relationship between actors and the roles they play is not static, but evolves with time and changing circumstances. Different actors have divergent characteristics and strengths. While state actors are the main providers of public goods, non-state actors are strong in their technical expertise and agenda-setting capabilities. What must be noted is that "[o]nly by giving the great powers pride of place is it possible to set the conditions under which non-state actors will exercise their influence."⁸

The driving force for the evolution of global governance in specific areas mainly comes from four sources: power shift in specific areas; major technological breakthroughs and diffusion in those areas; significant changes in the consciousness of actors in their political participation; and major changes in available resources that can be used for global governance.⁹ These factors decide how the roles and statuses of different actors in cyberspace will

China advocates the state's leading status in global cyber governance.

evolve, and can explain why cyber governance was dominated by technological elites at the early stages. With the rise of power, interest, resources, and especially awareness of a state, the primacy of the state in global cyber governance will keep growing.

⁷David Burt, Aaron Kleiner, J. Paul Nicholas, and Kevin Sullivan, *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*, Microsoft Corporation, 2014, pp. 1–50.

⁸Daniel W. Drezner, "The Global Governance of the Internet: Bring the State Back In," *Political Science Quarterly*, Vol. 119, No. 3 (2004), p. 498.

⁹Shi Chenxia, "A Theoretical Analysis of the Changes of Global Governance Pattern — A Case Study of Global Climate Change Governance," *Journal of International Relations*, No. 2 (2016), pp. 129–132.

Moreover, China's participation in global cyber governance is a process that transits from non-traditional security topics to a combination of non-traditional and traditional security issues. Cyberspace issues were generally considered as mainly concerning non-traditional security, which emphasizes social and human security — sometimes beyond the confines of the border. However, the understanding of cyberspace issues as basically non-traditional security issues may lead to a cyber governance dilemma: in the current international system, the situation of the state as the main security provider has not changed; yet in the meantime, it faces a growing diversity of security needs from within and the external environment, and thus it suffers from an increasing capacity shortage in security supply.

As it is, cyber security is a non-traditional security issue with obvious traditional security elements. From the perspective of non-traditional security, cyber-crime and cyber-terrorism have become common threats to human beings; in terms of traditional security, cyber security is related to national security, as information leaks and cyberattacks pose direct threats to military facilities and the intelligence system. In fact, cyberspace has become a "fifth battle field," after land, sea, air and space. The motivations behind various cyber threats are extremely complicated. They can be for military retaliation, political confrontation or over trade barriers; they may also be triggered by historical memory, identity differences and religious conflicts. In a word, non-traditional security problems can evolve into traditional security problems, and vice versa. To deal with cyberspace issues, not only are non-traditional security means utilized to meet traditional security concerns, but traditional security means are also employed to achieve non-traditional forms of security. Thus, traditional and non-traditional approaches are increasingly incorporated in cyber governance.

Finally, China's engagement in global cyber governance helps coordinate and integrate different values among nations. The global governance system of cyberspace includes five major components: the subject, the object, rules, values, and the results. Among them, values are the most important constructive force, which directly determines the efficacy of global cyber governance. The difficulty of value coordination arises from two factors: first, for each country, cyberspace problems are different in terms of form and degree, and values relating to cyber governance vary due to different social systems and levels of development. Second, even if a

consensus on values can be reached, there will likely be a difference in how these values are prioritized. For example, to many developing countries, freedom, equality and democracy are their long-term goals, but they are preceded by the necessity of survival and development.

In this sense, the rich philosophical legacy of the Chinese culture can help with the construction of values in global cyber governance. For instance, the notion of a “Community of Shared Future in Cyberspace” proposed by Chinese President Xi Jinping, which incorporates the traditional value of harmony, a common security prospect, a fair governance view and the concept of win-win development, can serve as an important supplement to the current understanding of global cyber governance. It is rooted in human virtue and aims to achieve peace and security of mankind. It also affirms the universal value of human unity, indivisibility and interdependence, which are fundamental to a harmonious cyber world. As the notion has been integrated into a resolution of the United Nations Human Rights Council,¹⁰ the “Community of Shared Future in Cyberspace” is likely to become a common value among all nations in global cyber governance.

China’s Basic Position and Approach

After more than two decades of rapid development, China has become a de facto cyber power. The number of Chinese netizens has grown to be the largest in the world. 7 of the top 20 most visited websites are based in China, and 6 of the 10 most popular social media sites are owned by China. In addition, 23 of China’s top 25 websites are products of Chinese Internet companies.¹¹ Nevertheless, China still has tremendous room for growth, for

¹⁰“Build a Community of Shared Future for Human Beings’ Written into United Nations Human Rights Council Resolutions for the First Time,” March 24, 2017, Chinese Mission to UN Office at Geneva, <http://www.china-un.ch/eng/dbtyw/rqrd.1/speech/t1448593.htm>.

¹¹Stephane Grumbach, *The Stakes of Big Data in the IT Industry: China as the Next Global Challenger?* (Paper prepared for the 18th International Euro-Asia Research Conference entitled “The Globalisation of Asian Markets: Implications for Multinational Investors,” held in Venezia, Italy from January 31 to February 1, 2013), pp. 5–7.

its Internet penetration rate has just passed 50 percent.¹² Such development and great potential have created basic conditions for China to participate more actively in global cyber governance.

There are many different interpretations of China's role in global governance. Gerrard Chen observes that from the perspective of international rule making, China has not developed enough capabilities to shape the structure of global governance.¹³ Scott Kennedy notes that China is taking on a reformative and progressive role in global governance, although it is generally satisfied and willing to maintain the status quo.¹⁴ Some other Western scholars note that the Chinese government has been focusing on improving the power balance in the field of global Internet technology governance in the past decade. Yet all these observations share one thing in common: they all agree that China has been playing an ever more active and important role in global cyber governance.

China's position on global cyber governance has two characteristics. One is its clear identity of a developing country. As Professor Wang Jisi of Peking University suggests, in participating in global governance, it is crucial that China should not only clarify but also stick to its identity as a developing country, and firmly stand alongside other developing countries.¹⁵ That is a point that runs through China's engagement in global governance in all fields. The other is China's endeavor to reform the various specific mechanisms while maintaining the existing global governance system. As China is one of the biggest beneficiaries of the current international order, there is no reason for China to revolutionize it. Rather, China

¹²On August 4, 2017, the China Internet Information Center (CNNIC) issued the 40th China Statistical Report on Internet Development. According to the report, as of June 2017, the number of Chinese netizens reached 751 million, accounting for one-fifth of the total number of Internet users in the world, and the Internet penetration rate is 54.3 percent. See http://cnnic.cn/gywm/xwzx/rdxw/201708/t20170804_69449.htm.

¹³Gerald Chan, Lee Pak K., and Chan Lai-Ha, *China Engages Global Governance: A New World Order in the Making* (London: Routledge, 2012).

¹⁴Scott Kennedy, "China in Global Governance: Why Kind of Status Quo Power?," in Scott Kennedy and Cheng Shuaihua, *From Rule Takers to Rule Makers: The Growing Role of Chinese in Global Governance* (Shanghai, Shanghai Longyu Printing Technology Co. Ltd, 2012).

¹⁵Wang Rengui, "Zhongguo tanlu quanqiuzhili," (China's Exploration in Global Governance) *Outlook Weekly*, June 6, 2011.

advocates an incremental approach to reform the global governance system.¹⁶ This position is reiterated in the official document, *International Strategy of Cooperation on Cyberspace of China*, which states that “China has been contributing to the building and maintaining of cyberspace.”¹⁷

Maintaining order is China’s primary consideration in domestic and global cyber governance.

Indeed, order — especially political order — is China’s primary consideration. As a Chinese scholar observes, China’s public policy regarding cyber governance always puts order first, innovation next, and security all the way through.¹⁸ The notion of order is not only rooted in the country’s cultural background and national conditions, but it is also behind China’s advocacy of the concept

of cyber sovereignty. Thus, China’s participation in global cyber governance is a process of exploration with a sort of “patch-work” approach. In the meantime, China is increasingly becoming involved in different aspects of global cyber governance.

First of all, China’s engagement in global cyber governance has become more extensive over the past decade. China not only actively participates in the international policy making process dealing with such topics as cooperative technological standards, information and communication technology industries, fighting against cyber-crime, as well as digital economy and digital divide, but it also pays more attention to national security, political security, economic security and social security issues in the context of the flourishing cyberspace.

Second, China’s involvement in cyber affairs covers bilateral, regional, multilateral and international levels. Bilaterally, China has established inter-governmental dialogue and cooperation mechanisms with South Korea, the UK and Australia. In May and December 2016, the 2nd and 3rd

¹⁶Huang Chao, “A Review of the Theory of China’s Participation in Global Governance,” *Journal of International Relations*, No. 4 (2013), pp. 65–66.

¹⁷*International Strategy of Cooperation on Cyberspace*, jointly released by Ministry of Foreign Affairs and Cyberspace Administration of China on March 1, 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

¹⁸Sun Yu and Feng Lishuo, “Changing Logic of Chinese Internet Governance Policy During 1994–2014,” *Journal of Intelligence*, Vol. 36, No. 1 (2017), pp. 87–91.

U.S.-China Cybercrime and Related Issues High Level Joint Dialogue were held in Washington, D.C. In June of that year, China and Russia issued the "Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development."

At the regional level, there are various dialogue and cooperation mechanisms on the Internet and cyber-crime between China and the Association of Southeast Asian Nations (ASEAN), the Shanghai Cooperation Organization (SCO), other BRICS countries (Brazil, Russia, India and South Africa), the European Union (EU) and the League of Arab States (LAS). For instance, in early 2009, the Chinese government signed a co-operation agreement with the ASEAN Telecommunications Regulatory Council on network security issues.¹⁹ In the same year, China and other SCO member states reached an agreement for cooperation in ensuring international information security, which was reiterated on the SCO summit on June 9, 2017.²⁰

At the multilateral and international levels, China has been playing a significant role in such mechanisms as the Group of Governmental Experts on Information Security (GGE) convened under the auspices of the United Nations, the International Telecommunication Union (ITU), the World Summit on the Information Society (WSIS), the Cyber Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Asia-Pacific Internet Information Center (APNIC), the Internet Society (ISOC), and the Internet Architecture Board (IAB), among others. Besides, by hosting the World Internet Conference, China has been developing its own stance on cyber diplomacy as well.

Third, in terms of actors, the Chinese government encourages the private sector and civil society to participate in various global cyber governance mechanisms. Furthermore, China's official participation has extended from traditional government bodies like the Ministry of Foreign Affairs (MFA) and Ministry of Industry and Information Technology

¹⁹"China-ASEAN Cooperation: 1991–2011," November 16, 2011, <http://cpc.people.com.cn/GB/64093/64387/16267873.html>.

²⁰"The Agreement of SCO on Cooperation in the Field of Ensuring International Information Security" was first signed in 2009, and further confirmed in the 2017 SCO summit declaration, http://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t1469140.shtml.

(MIIT) to other bodies, such as the Ministry of Public Security (MPS), Ministry of Commerce (MOFCOM), Ministry of Finance (MOF), and the newly established Cyberspace Administration of China (CAC). The MFA also set up a special office on cyberspace affairs to address diplomatic issues concerning cyberspace.

Fourth, having realized the importance of “top-level design,” China is moving from strategic ambiguity to strategic clarity on cyber governance, which can be seen from the many official statements and legal documents issued over the past few years. Since 2016, China has put forward four major laws and documents, including the *Cybersecurity Law*,²¹ the *National Cybersecurity Strategy*,²² the *Outline of National Informatization Development Strategy*,²³ and the *International Strategy of Cooperation in Cyberspace*.²⁴ As its cyber capacity continues to grow, China has become more confident in clarifying its position and strategy in cyber governance.

Reviewing the above-mentioned laws and policy documents, together with President Xi’s related remarks as well as Chinese and international research literature on China’s practices in international cyber activities,

the Chinese approach to global cyber governance can be further summarized as one of multilateral pluralism based on cyber sovereignty, which includes the following aspects:

Most importantly, China is determined to defend its cyber sovereignty and ensure its national security. In the eyes of many

Mutual respect for cyber sovereignty is China’s fundamental principle in global cyber governance.

²¹*The Cybersecurity Law of the People’s Republic of China*, adopted at the 24th meeting of the Standing Committee of the 12th National People’s Congress on November 7, 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

²²*National Cybersecurity Strategy*, approved by the Central Leading Group for Cyberspace Affairs and released by the Cyberspace Administration of China on December 27, 2016, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

²³*National Information Development Strategy Outline*, issued by the Office of the State Council of China on July 27, 2016, http://www.gov.cn/zhengce/2016-07/27/content_5095336.htm.

²⁴*International Strategy of Cooperation on Cyberspace*.

Western scholars, cyber sovereignty (or Internet sovereignty) is the core idea of China's cyber governance, from which other positions are derived.²⁵ As early as 2011, China, together with Russia and several other nations, submitted to the United Nations a document entitled "International Code of Conduct on Information Security," in which they proposed that policy and decision-making on cyber governance is part of each country's sovereignty; the principle was reiterated in the updated version of the document in 2015.²⁶ Yet the concept of "cyber sovereignty" was put forward explicitly for the first time only in the *National Security Law of the People's Republic of China*, promulgated on July 1, 2015, and was elaborated by President Xi in December 2015:

*The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security.*²⁷

Afterwards, cyber sovereignty was also highlighted in China's *Cybersecurity Law*, the *National Cybersecurity Strategy*, and the *International Strategy of Cooperation in Cyberspace*.

²⁵Hong Shen, "China and Global Internet Governance: Toward an Alternative Analytical Framework," published online, July 12, 2016, <http://www.tandfonline.com/doi/abs/10.1080/17544750.2016.1206028?journalCode=rjc20>.

²⁶*International Code of Conduct for Information Security*, http://infogate.fmprc.gov.cn/web/ziliaoj_674904/tytj_674911/zcwj_674915/P020150316571763224632.pdf.

²⁷Xi Jinping's Remarks at the Opening Ceremony of the 2nd World Internet Conference, Wuzhen, China, December 16, 2015, http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zjyh_665391/t1327570.shtml.

Although cyber sovereignty has become a “de-facto reality for every country,”²⁸ China attaches particular significance to the notion of cyber sovereignty mainly for four reasons.

The most important reason is that the notion is rooted in numerous national crises that China has experienced in history. China’s colonial experience in the 19th and 20th centuries, the Western interference in Taiwan, Tibet, and Xinjiang affairs, as well as human rights issues have led China to all the more cherish its national independence and state sovereignty.²⁹ Currently, the global cyber governance system — whether in terms of Internet resources, technological standards, international norms, or power of discourse — is still dominated by Western countries. Thus, China believes it is necessary to employ the notion of cyber sovereignty, in order to protect itself from being eroded by Western influence and to strive for more cyber governance rights for developing countries. China’s unique national conditions, featured by its cyberspace censorship, also require the notion as a basis of its policy deliberation.

The second reason is that China has emphasized the leading role of the state and the United Nations in global cyber governance, which is shown in its *International Strategy of Cooperation in Cyberspace*:

*China supports formulating universally accepted international rules and norms of state behavior in cyberspace within the framework of the United Nations. . . Relevant efforts should reflect broad participation, sound management and democratic decision-making, with all stakeholders contributing in [sic] their share based on their capacity and governments taking the leading role in Internet governance particularly public policies and security.*³⁰

A review of global cyber governance indicates that, although the state is not the only actor, it is playing an irreplaceable role in global cyber governance, especially in the field of public policy and national security. This is because

²⁸Liu Yangyue and Yang Yixin, “The Resurgence of Sovereignty in Cyberspace and Its Implications for Cyber Governance,” *International Forum*, No. 6 (2013), pp. 1–7.

²⁹Zhao Chen, “A Comparative Study of Global Governance Concepts of EU, US, and China,” *The Journal of International Studies*, No. 3 (2012), pp. 101–102.

³⁰*International Strategy of Cooperation on Cyberspace*.

it remains the biggest owner of legitimacy and responsibility under law, and it is the most effective force for the implementation and promotion of global governance. To be more specific, the power of the government lies in its political authority, which allows it to pool resources, provide necessary public goods, and put forward comprehensive plans through policies, regulations, publicity and other means, so as to create the needed environment and conditions for governance. For instance, in the face of many unexpected security threats in cyberspace, the government is the only actor that can respond with timely countermeasures; in international cooperation, the government is also the only player representing the overall interest of a country rather than vested interest of a particular group.

That said, China has supported the pragmatic participation of other actors in global cyber governance when it perceives that as beneficial, or at least not harmful, to its national interest and not a challenge to the government's authority.³¹ As stressed in the *International Strategy of Cooperation in Cyberspace* (in the section named "Promoting Fair Governance"):

China's non-state actors play a limited and complementary role to the government in global cyber governance.

*International cyberspace governance should feature multiparty participation and all parties, including governments, international organizations, Internet companies, technology communities, non-governmental institutions and individuals, should play their respective roles in building an all-dimensional and multi-tiered governance platform.*³²

In practice, Internet business groups and technological elites are both encouraged to play a complementary role in China's overall engagement in global cyber governance. For example, China withdrew from the

³¹Huang Xu, "Analysis of the Process and Driving Force on Participating in the Global Cyber Governance Organization: A Case Study of the Internet Engineering Task Force," *Journal of Hunan University of Science & Technology (Social Science Edition)*, Vol. 19, No. 5 (September 2016).

³²*International Strategy of Cooperation on Cyberspace*.

transnational Government Advisory Committee (GAC) in 2001 and did not rejoin it until 2009. During the absence of the government, China's private sector, civil society and even individuals continued to participate in ICANN activities.³³ As another example, Jack Ma, Chairman of the Alibaba Group, as the sole representative of the private sector in Asia and Oceania, was elected in January 2015 as a member of the Global Cyber Governance Alliance (GIGA) Committee.³⁴ It is believed that China allows the participation of non-state actors mainly to enhance the government's capabilities and to counterbalance the U.S. supremacy in the global Internet technology governance system.³⁵

The third reason is that although China embraces the common principles of multilateralism, democracy and transparency in global cyber governance, it tends to interpret them differently from Western countries. While developed countries generally interpret multilateralism as support for the participation of multi-stakeholders, including non-profit organizations, China places more emphasis on equal participation of all governments in policy making. In the context of cyber governance, democracy as perceived by Western countries focuses on the domestic level, such as the free flow of information and the users' right to participate in the decision-making process. Yet democracy advocated by China mainly refers to international affairs in that China has been opposing the monopolization of cyber governance by Western countries and strongly safeguarding state sovereignty, in order to avoid unequal participation between developed and developing countries for their different levels of Internet development. In terms of transparency, the United States and other Western countries advocate a free and open network environment, and focus on the transparency of network management. By contrast, China's understanding of transparency focuses on international rules; it calls for transparent rules in global cyber governance so that developing countries share equal rights with developed ones in the governance process.

The fourth reason is that China regards the development of national power and domestic governance practices fundamental to a country's

³³Galloway and He, "China and the Global Internet Technological Governance."

³⁴The Global Cyber Governance Alliance (GIGA) Committee was jointly initiated by the ICANN, the Brazil Internet Steering Committee and the World Economic Forum.

³⁵Galloway and He, "China and the Global Internet Technological Governance."

participation in global governance. Recognizing that the U.S. hegemony over the Internet is largely attributed to its dominant national power, especially technological strength, China has taken tremendous efforts to promote the development of Internet-related technologies. The “Internet-plus” strategy is a case in point. First proposed by Mr. Yu Yang, Chairman and CEO of Analysis International, in November 2012, and formally advocated by Premier Li Keqiang in his work report to the 12th National People’s Congress in March 2015, the strategy aims to promote the integration of mobile Internet, cloud computing, big data, and Internet of things (IoT) with modern manufacturing industry, as well as the development of e-commerce, industrial Internet and Internet finance (ITFIN).³⁶

China also attaches great importance to the training of technical, legal and policy professionals, as well as other related talents, and is scaling up research investment on domestic cyber governance. Cyber security has been added to the list of highest-level disciplines by the Ministry of Education (MOE), and many universities have set up schools and research centers focused on the issue. All these help improve China’s overall representation and influence in global cyber governance. As a result, an increasing number of individuals from Internet companies, civil organizations and academic institutions are actively participating in such international organizations as the ICANN, IETF and IAB.

Understanding the Gap between China and the West

China’s engagement in global cyber governance has incurred much doubt from the international community, especially Western countries. Despite the sincere attitude and policy elaboration by the Chinese government, there remains much misunderstanding about the basic principles it has followed over the years, such as its reluctance to adopt a multi-stakeholder governance approach, its strong support for global governance under the UN framework, and its advocacy for government-led multilateralism. Many countries are also concerned about the notion of “cyber sovereignty,” which they believe would contradict the global commons, Internet freedom,

³⁶The State Council of the People’s Republic of China, “Premier Li and Internet Plus,” Dec 31, 2015, http://english.gov.cn/policies/infographics/2015/12/31/content_281475263938767.htm.

and the “Community of Shared Future in Cyberspace” proposed by China itself.

Indeed, whether to follow a multi-stakeholder or multilateral approach has been under debate since the early stage of global cyber governance, in large part due to a lack of common understanding of the two concepts. The habitual over-simplification of academic studies and expert reports also adds to the confusion.³⁷ Besides, the concept of “multi-stakeholder” carries with it such an inborn political correctness that it has prevented any sober assessment of whether or not the concept is confusing in itself.³⁸

There is no clear definition of the “multi-stakeholder” approach, but its essence is simple and clear: for one, it aims at a “non-centralized and distributed power balance,”³⁹ with the government, the private sector, the non-governmental organizations and other actors involved on the same footing; for another, the multi-stakeholder approach has already manifested itself in different forms across different areas.⁴⁰ As

The multi-stakeholder and multilateral approaches complement each other in practice.

Laura DeNardis, a famous American professor in cyber governance studies, observes, there are at least three alternative forms of the multi-stakeholder approach, namely, the “widely distributed” model, the “government-led” model, and the “private sector-led” model.⁴¹ In a sense, multilateralism is also a form of the multi-stakeholder approach.

China does not oppose the multi-stakeholder approach, and it has neither the intention nor capability to challenge this approach. “Multilateral pluralism” may be a more appropriate term for China’s stance. China has made it clear that it encourages “enhanced communication and cooperation

³⁷Gady, “The Wuzhen Summit and the Battle over Internet Governance.”

³⁸Laura DeNardis, *Global War for Internet Governance* (Beijing: China Renmin University Press, 2017), p. 256.

³⁹*Ibid.*, p. 257.

⁴⁰Lang Ping, “The ‘Multi-Stakeholder’ Approach to Cyber Governance from the Perspective of Global Governance,” *Contemporary International Relations*, No. 4 (2017), pp. 47–53.

⁴¹DeNardis, *Global War for Internet Governance*, p. 255.

among all stakeholders" to "contribute [in] their share based on their capacity".⁴² In other words, the Chinese government does not exclude participation and monitoring from other actors. Therefore, the multi-stakeholder approach and the multilateralism/multilateral pluralism approach are not mutually exclusive, but rather complementary to each other.⁴³ Although the former advocates no central authority as well as an inclusive and networked decision-making process, while the latter tends to emphasize the relatively dominant position of governments among various stakeholders, they both engage multiple actors in cyber governance.

The next conflicting topic is cyber sovereignty. As a matter of fact, cyberspace is neither part of the global commons, nor a completely domestic domain, but a mixed common pool of resources.⁴⁴ The global commons is generally understood as the field where no single country is able to enjoy exclusive sovereignty, such as the oceans, outer space and the Antarctic.⁴⁵ To the U.S. strategic circle, there are mainly four areas that can be so called: the high seas, outer space, international airspace and cyberspace.⁴⁶ However, not all Western scholars see cyberspace part of the global commons, instead, many regard it as an artificial creation which rests on a tangible, physical construct.⁴⁷ For example, Joseph Nye believes that since cyberspace is, to a large extent, under the control of sovereign states, it is not a field similar to the high seas.⁴⁸ In fact, the notion of cyberspace as part of the global commons undercuts both national and international security and it is increasingly unsustainable as some governments seek technological and policy solutions to extend their control in cyberspace.⁴⁹

⁴²International Strategy of Cooperation on Cyberspace.

⁴³Lang, "The 'Multi-Stakeholder' Approach to Cyber Governance from the Perspective of Global Governance."

⁴⁴Scott J. Shackelford, "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance," *American University Law Review*, Vol. 62, No. 5 (2013), p. 1322.

⁴⁵OECD, "Glossary of Statistical Terms," <http://stats.oecd.org/glossary/detail.asp?ID=1120>.

⁴⁶U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Department of Defense, 2010).

⁴⁷James Lewis, "Sovereignty and the Role of Government in Cyberspace," *Brown Journal of World Affairs*, Vol. 16, No. 2 (Spring/Summer 2010), p. 62.

⁴⁸Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011), p. 143.

A third topic regards such values as “Internet freedom” and “human rights in cyberspace.” Actually, a main concern of the West about China’s notion of cyber sovereignty is its potential incursion into the private lives of citizens and its hindrance to the free flow of information. China’s Internet censorship and stringent government measures to control the Internet are often criticized from the perspective of international human rights law and international trade law. For instance, Amnesty International warns that China’s cyber sovereignty may cause an infringement upon the right of freedom of expression, and thus calls on the big IT companies like Apple, Google, Facebook, LinkedIn and Microsoft to say no to China’s “repressive Internet regime.”⁵⁰

Admittedly, the rapid evolution of the Internet has greatly promoted the freedom of cyberspace. The very nature of real-time interactivity, transnationality, anonymity and virtuality of the Internet have all provided the public with freedom of speech to the utmost extent. However, the role of the Internet in information freedom is not entirely positive, due to the fact that some actors can manipulate Internet norms for bad or even evil purposes, such as piracy of intellectual property rights (IPRs), theft of secrets, libel, and invasion of privacy, which create new threats to the basic rights and freedom of other citizens.

In this sense, the so-called “Internet freedom” is not that free in any country. There are externalities, or side effects, of all human behaviors.

Cyber sovereignty is necessary when Internet freedom needs protection by the state.

Unless such externalities are effectively contained, it will be very difficult for human beings to live peacefully, and the result may be a “tragedy of the commons” — a situation where all suffer because each individual acts independently out of his or her self-interest. Thus, public interest, such as public stability or security, needs to be prioritized over the concern of free flow of information.

⁴⁹Lewis, “Sovereignty and the Role of Government in Cyberspace,” p. 56.

⁵⁰Roseann Rife, “Tech Companies Must Reject China’s Repressive Internet Rules,” Amnesty International, December 15, 2015, <https://www.amnesty.org/en/latest/news/2015/12/tech-companies-must-reject-china-repressive-Internet-rules/>.

In John Stuart Mill's words, people "have a responsibility to act on behalf of public interests rather than 'private partialities.'"⁵¹ Mainly in the field of national security, public interest must be protected by the state through its adherence to cyber sovereignty.

The last topic is the Chinese notion of a "Community of Shared Future in Cyberspace." Proposed by President Xi in his keynote speech at the 2nd World Internet Conference held in December 2015, the notion has become a buzzword in China. In his speech, President Xi made five specific proposals for building a "Community of Shared Future in Cyberspace": (1) to speed up the construction of global network infrastructure and promote inter-connectivity; (2) to create an online platform for sharing cultural exchanges and promoting mutual exchange; (3) to promote innovation and development of the Internet economy as well as common prosperity; (4) to safeguard network security and promote orderly development; and (5) to construct a cyber governance system of fairness and justice.⁵² During the 3rd World Internet Conference in November 2016, President Xi further advocated the principles of "equality and respect, innovation and development, openness and sharing, security and order" in cyber governance.⁵³

However, the sincerity of China's proposal to build a "Community of Shared Future in Cyberspace" is often questioned by the West, mainly due to the Chinese government's persistence in cyber sovereignty. Yet, according to the modern theory of sovereignty, the nation state still lies at the center of national rationality, which suggests that the state must utilize any possible means to protect and maintain its self-interest, be it political stability or public order. Scholars like Niccolò Machiavelli, Jean Bodin, and Thomas Hobbes all held this view. As a developing country, China has no choice but to adopt this rationale.

⁵¹Paul Starr, *Freedom's Power: The True Force of Liberalism* (New York: Basic Books, 2007), p. 58.

⁵²Address by President Xi Jinping at the opening ceremony of the 2nd World Internet Conference, Wuzhen, China, December 16, 2015, http://www.cac.gov.cn/2015-12/16/c_1117481112.htm.

⁵³The video address was given by President Xi Jinping at the opening ceremony of the 3rd World Internet Conference, Wuzhen, China, November 16, 2016, http://news.xinhuanet.com/politics/2016-11/16/c_1119925133.htm.

In reality, the misunderstanding of the West on the relationship between cyber sovereignty and the “Community of Shared Future in Cyberspace” originates, on the one hand, from a failure to take into account the self-restriction of the state and the relativity of sovereignty, which can be transferred when circumstances allow; on the other hand, it is because unlike China, the West would not see the building of a “Community of Shared Future in Cyberspace” as a long and lasting process. From a Marxist perspective, national sovereignty is both a historical legacy and a necessary stage to achieve the comprehensive development of human society.⁵⁴ Thus, mutual respect for cyber sovereignty and jointly building a “Community of Shared Future in Cyberspace” can be dialectically unified.⁵⁵

Conclusion

China’s growing strength and stake in cyberspace have made it an active and important actor in global cyber governance. Over the past decade, China has participated in the global governance process in a way that conforms to its national identity as a developing country, and its contribution has been appreciated by the vast developing world, which shares similar needs to safeguard national sovereignty and domestic order, as well as to seek a bigger say in international affairs.

In general, China’s approach to global cyber governance can be described as one of multilateral pluralism, indicated by four main points: to safeguard cyber sovereignty and ensure national security; to stick to the government’s dominant role while pragmatically supporting other actors in global cyberspace governance; to enhance multilateralism, democracy and transparency in cyberspace on an interpretation that fits its national realities; and to make every effort to develop its national power, including technological strength, and enhance domestic governance of the Internet.

⁵⁴Che Yueli, “Contemporary Thinking on the Principle of State Sovereignty — A View from Marx Doctrine,” *Theory and Reform*, No. 4 (2002), pp. 21–25.

⁵⁵Lu Wei, “Adhering to the Principle of Respect for Cyber Sovereignty and Promoting the Construction of a Community of Shared Future in Cyberspace — A Reflection on Learning, Xi Jinping’s Speech at the Second World Internet Conference,” *China Information Security*, No. 3 (2016), p. 36.

As a rapidly emerging power, China is expected to become more deeply involved in global cyber governance as a constructive and responsible stakeholder. Meanwhile, it will keep enhancing its cyber capacity and domestic governance model, so as to play a bigger part in the global arena. With more engagement from China and other developing countries, an in-depth, effective, rational and harmonious governance approach will lead the future direction of global cyber governance.