International Relations and Diplomacy, January 2018, Vol. 06, No.01, 16-23
doi: 10.17265/2328-2134/2018.01.002

An Analysis of Cyberspace Rule-Making in China-U.S. Relations

Zhao GENG
Shanghai International Studies University, Shanghai, China

As an established power and a rising power respectively, the U.S. and China have profound impacts on the development of cyberspace. The foundation of cyberspace governance is to constrain the behavior of every international actor with effective norms. Therefore, cyberspace rule-making has an important implication in China-U.S. relations and it is necessary for both sides to formulate cyberspace norms under mutually acceptable concepts. Besides, the ideas of "a new type of major power relations" and "a community with a shared future for mankind" provide theoretical foundation for cyberspace rule-making. In the short term, the establishment of norms can be promoted by negotiating limited issues, which could be called a low-level path. In the long run, they will reach informal mechanism which can be called a middle-level path, as well as formal mechanism of mutual recognition which can be seen as a high-level path, promoting the enforcement of cyberspace norms. Besides, "Track Two Diplomacy" and "Track 1.5 Diplomacy" also benefit the process of cyberspace rule-making negotiations.

Keywords: cyberspace, rule-making, Sino-U.S. relations

Introduction

The wide application of internet technology affects the development of human beings deeply. At the same time, the disorder and confusion in cyberspace also lead to new problems and challenges for contemporary international relations. Effective institution and stabile order are essential to the area and it is really necessary for cyber major powers to formulate acceptable rules. Nowadays, China and the U.S. have become leading powers in cyberspace and they will affect global cyberspace rule-making greatly. The paper aims to illustrate the backgrounds and present situation of China-U.S. cyberspace rule-making, and puts forward feasible paths and methods for both sides to constitute cyberspace norms.

The Background of Cyberspace Rule-Making

In face of hacker attack, cyber war, cyber terrorism, cyber spying and so on, the formulating of cyberspace norms has become an important issue in bilateral and multilateral diplomacy, especially major power relations. In the history of international relations, from Westphalian System to present, regime and institution have taken important positions in international relations. As neo-liberalists said, regimes are a kind of rules recognized by all international relations actors. These actors reach mutually agreements and abide them. Especially on multilateral diplomacy, working well characteristically regimes can facilitate burden sharing and provide

Zhao GENG, Ph.D. Candidate, School of International Relations and Public Affairs, Shanghai International Studies University.

information to governments (Robert & Joseph, 2010, p. 285). Therefore, in international politics, international institutions can usually be regard as an effective method for dealing with international disputes. Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action (Stephen, 1982, p. 186).

The usage of internet was from military affairs and scientific research to both military use and civilian use since 1990s. The U.S. has a large impact on non-governmental organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN). Russia firstly put forward the proposal which is different from the U.S. about cyberspace in general assembly of the United Nations (UN). It can be a prelude for the U.S. and other countries' disputes on cyberspace. China and Russia have different points of view about cyberspace rules with western countries and they believe that cyberspace governance should follow the principle of "government dominance". However, the U.S. put forward that the man body of cyberspace should be "multiple stakeholders" which refers to government, social group, individuals and so on.

The western countries have made a progress on making cyberspace rules. In March 2013, the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence invited 20 experts to edit the Tallinn Manual. Although the manual is just a recommended handbook, not the official document or policy of NATO. It can be regard as the first systematic international cyber law. It defines some key concepts on cyber war, pointing to the core issues in cybersecurity. It regulated that in cyberspace, an internationally wrongful act can consist, inter alia, of a violation of the United Nations Charter or a violation of a law of armed conflict obligation attributable or the state in question. A breach of peacetime rules not involving conflict also constitutes an internationally wrongful act (Michael, 2013, pp. 29-30). Due to advanced internet infrastructure and similar values, U.S. and EU have reached much consensus on the formulation of norms, and they have promoted close cooperation.

As a result, current cyberspace rule-making is still in initial phase called "proposed norms". The cooperation among countries focuses on combating cyber terrorism and cybercrime. The normal cyber conflict and cyber war show the competition and game among states. The current game among countries manifests the conflicts of governance patterns between U.S.-EU and China-Russia, as well as the competition for dominant position between the U.S. and the EU (LANG, 2015, p. 129).

Current Situation of Cyberspace Rule-Making Between China and U.S.

The Differences on Understanding Several Cyberspace Concepts

China and U.S. hold different views on the definition of cybersecurity and cyber sovereignty. In addition, the two countries have different cyber strategy. Firstly, China and the U.S. have formed their different understanding on the definition of cybersecurity. If the two countries don't have consensus on the concept, they will don't deal with the issues in cyberspace effectively, not alone cooperate in the issue and formulate mutually acceptable norms. On the view of the U.S., cybersecurity is fundamentally about preventing unauthorized access to digital systems and, notwithstanding massive foreign hacking of U.S. government databases, mainly focuses on protecting private-sector data as well as critical infrastructure (Zachary & Jerome, 2016). Besides, U.S. government highlights that cyberspace crosses every international boundary. It must engage with our international partners and work to create incentives for, and build consensus around, an

international environment where states recognize the value of an open, interoperable, secure, and reliable cyberspace. It will oppose efforts to restrict internet freedoms, eliminating the multi-stakeholder approach to internet governance, or impose political and bureaucratic layers unable to keep up with the speed of technological change. An open, transparent, secure, and stable cyberspace is critical to the success of the global economy (The White House, 2016).

However, the basic concept of China's cybersecurity concept is based on state-centric, safeguarding against digitally enabled threats to the regime, internal and external. China seeks what it calls "cyber-sovereignty", a term loosely understood to entail significant control over the internet, including over the content of online information (Zachary & Jerome, 2016). Cybersecurity is defined by *Cyber Security Law of the P.R.C.*as taking necessary measures to prevent cyber-attacks, incursions, interference, destruction, and their unlawful use, as well as unexpected accidents; to put the networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable (Ministry of Industry and Information Technology of the P.R.C., 2016).

Therefore, on the definition of cybersecurity, rather than conceptual interpretation in the technical level, the difference of political institution, economy, and culture influent the understanding of cybersecurity. As the mechanism of enforcement and cybersecurity dialogue has been established in XI-Trump Era, China and the U.S. have more probabilities to reach consensus on the concept of cybersecurity which needs the bilaterally mutual trust. It would be a long time process.

Secondly, on the concept of cyber sovereignty, the two sides have formed different viewpoints. As for China, cyber sovereignty mainly includes four aspects. Jurisdiction refers to the power of the sovereign state to manage cyberspace. The defense power is for the sovereign state to defend against the cyber-attacks and threats. The independent power is ensuring the independent operation of the national cyberspace. Equality power refers to sovereign states participating equally in the global cyber governance (HUAN, 2016, p. 5). In contract, the U.S. believes that cyber sovereignty only can be applied to the jurisdiction of key information infrastructure and relevant entrepreneurs' activities within the domestic territory. It is not permitted to impede cross-border data flows and other activities related to the effective interconnection in global cyberspace.

China's interpretation on the applicability of the cyber sovereignty will lead the U.S. to increase its bias against China in a short period. But in the long run, cyber sovereignty is an important means for China to effectively protect national cybersecurity. As a result, China should actively dialogue and coordinate with western countries and clarify its understanding on cyber sovereignty and explain the concept's legitimacy. The proposal of this concept will promote China's cyber industry development, and it will benefit China's participation in global cyberspace rule-making.

Thirdly, on cyberspace strategy, China and the U.S. also contain some diversities. China released its first national cyber strategy in December 2016, and the strategy illustrates and reaffirms China's main positions and propositions on cyberspace development and security and serves as the guide for China's cybersecurity work. The strategy aims to build China into a cyber-power while promoting an orderly, secure, and open cyberspace and safeguarding national sovereignty (United States Information Technology Office, 2016). In addition, China also listed its major tasks in this area, which are the defend cyberspace sovereignty; protect national security; protect critical information infrastructure (CII); build a healthy online culture; fight cybercrime, espionage, and terrorism; improve cyber governance; enhance baseline cybersecurity; elevate cyberspace defense capabilities; and strengthen international cooperation respectively (CAC, 2016). Concerning the U.S., based on the cyber

strategy issued by Department of Deference (DoD), it focuses on building cyber capabilities and organizations for DoD's three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyber attacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans (U.S. Department of Defense, 2015).

To conclude, the overall goal of cybersecurity in China is to protect and maintain the security of cyberspace so as to guarantee the security and stability of Chinese political, economic, and social stability. As for the U.S., except maintaining the security of the internet hardware and software, its cybersecurity goal is to maintain the global network order, lead to the development of the global network space, and maintain its absolute superiority in cyberspace. Therefore, the differences between China and the U.S. make the two countries learn more each other's interests in this area and build strategic mutual trust to some degree.

Bilateral Cybersecurity High-Level Dialogue Mechanisms Continue Making Progress

In 2013, the first meeting of China and U.S. presidents interfered with cybersecurity issue. Both sides decided to establish cyber working group in the framework of China-U.S. Strategic Security Dialogue, continuing negotiating on the issue. They should eliminate suspicion and cooperate to promote cybersecurity becomes a new bright spot in Sino-U.S. relations (DU, WU, & CHEN, 2013).

Afterwards, in the outcome list of 2015 president XI's state visit to the U.S., cybersecurity issue had been put in an important position. Both sides agreed that timely responses should be provided to requests for information and assistance concerning malicious cyber activities, as well as cooperating in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from their territory. Both sides also agreed to provide updates on the status and results of those investigations to the other side, as appropriate. Besides, they were committed to making common efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community (Ministry of Foreign Affairs of the P.R.C., 2015). The two sides also consented to create a senior experts group for further discussions on this topic and establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China would designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the Attorney General would co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides admitted to establish a hotline for the escalation of issues that may arise in the course of responding to such requests (Ministry of Foreign Affairs of the P.R.C., 2015). In addition, relevant departments of the two countries agreed to enhance case investigation and information sharing. They will not support the behavior of cyber theft on intellectual property rights and discuss to promote formulating national behavior in cyberspace (ZHENG & HUANG, 2015). The both sides also would hold two dialogues discussing related issues. Therefore, as a detailed level in cyberspace, China and the U.S.' cooperation on combating cybercrime will build a new model for other cybersecurity issues.

This co-chair high-level dialogue can be transformed and promoted. In April 2017, President XI met Trump in Mar-A-Lago, the four high-level joint dialogue mechanisms have been put forward. Enforce and cybersecurity dialogue has become an important one in this new mechanism. In October 2017, the first enforcement and cybersecurity dialogue was held in Washington. On the rule-making issue, both sides agreed to make common efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community (Homeland Security, 2017).

From a series bilateral dialogues and negotiations in recent years, China and the U.S. have noticed the importance of cyber issues in bilateral relations. Because the appearance time of cyber issues is late, both sides' consensus on the issue is too general, and they have not reached a deep level in this field (e.g., a series of concepts definition, the fundamental rule-making on cybersecurity and standard settings about Internet soft-hardware). The above issues will be discussed by China and U.S. relevant departments in the future.

The Prospect of Cyberspace Rule-Making in China-U.S. Relations

Cyberspace Rule-Making Under the Guideline of "a New Type of China-U.S. Major Power Relations" and "a Community With a Shared Future for Mankind"

During President XI's state visit to the U.S. in 2013, he summarized the concept of "a new type of China-U.S. major power relations", which is based on no conflict, no confrontation, mutual respect, and win-win cooperation. In this framework, the formulation of cyberspace norms becomes a realistic problem in the bilateral relations. The negotiation and dialogue on cyberspace rules can be a model of justice and equality. The U.S. has formulated relevant rules which are beneficial to its own, and it naturally doesn't hope that China will challenge its major position in cyberspace. Therefore, China needs to negotiate with the U.S. in the concept of mutual respect. Mutual respect means respecting each other's choice for social system and path of development, as well as each other's core interests and major concerns, seeking common ground while reserving differences, tolerance and mutual learning to common progress (The Central People's Government of P.R.C., 2013). The U.S. hopes that other countries can accept its cyberspace norms. On the basis of its cyber norms' foundation, the U.S. can deterrent and contain the potential violators. The U.S. may follow the mechanism on preventing the diffusion of mass destructed weapons, putting cybersecurity issues into bilateral and multilateral plans (DU, 2013, p. 164). Besides, China put forward the concept called "a community with a shared future for mankind" which means that a country should accommodate the legitimate concerns of others when pursuing its own interests; and it should promote common development of all countries when advancing its own development (Xinhuanet, 2012). The concept is a new and important public good for the world and it provides solutions for global governance.

In cyberspace, the concept has more suitable range. The virtual nature of cyberspace can reflect that it is served for the mankind. Therefore, keeping national interests in this area, China and the U.S. can stand on a higher stage for the human's future to promote the development of cyberspace. Cyberspace rule-making needs understanding and respecting mutual intentions and strategic objectives. In the negotiation, the two sides should make certain compromises and concessions. As a result, it is necessary for related experts to participate in establishing mutual acceptable cyberspace norms. Besides, carbon emissions, climate change and other international issues' negotiation also can provide experience or enlightenments for cyberspace rule-making.

Three Paths for China-U.S. Cyberspace Rule-Making

During XI Jinping's state visit to the U.S. in 2015, China and the U.S. has reached consensus on negotiating cybersecurity by expert groups. The bilateral high-level personnel consultation meetings are helpful to comprehend each other's intentions. The two countries should also come up with corresponding solutions in the issues of hacker attacks, cyber-crime, cyber terrorism, and cyber war, regulating above problems in the field.

The first one is a low-level path. It means that China and the U.S. build limited norms in cyberspace such as fighting cyber transnational crime. But their cooperation area is limited. It is a microcosm of China-U.S. structural contradictions in cyberspace that U.S. sued Chinese military officers for cyber theft in 2014. The contradiction indeed hinders the current bilateral dialogue and cooperation in the field of cyberspace. Although it is hard for two countries to dispel contradiction in cyberspace, with the Sino-U.S. consultations on the heads of state visits, strategic and economic dialogue, the internet conference and a series of bilateral and multilateral occasions, it is probable to cooperate in limited aspects. For example, in combating cybercrime, China and the U.S. have reached some relevant guidelines. At the same time, they have agreed to build hotline for cybercrime and related issues to communicate directly with each other on major emergency cases in cyberspace and cyber law enforcement cooperation, so that they can deal with the upgrade problems in response to these requests. Besides, the two sides also agreed to cooperate on this issue, including cyber dissemination of child pornography, commercial theft, online fraud, and online terrorist activity. As the same time, they will strengthen the sector exchanges in cyberspace protection under the mechanism (Ministry of Police, 2016).

The second one is a middle-level path. That is to say, the two countries could formulate informal norms in cyberspace. The active function of informal norms benefits creating a common concept of responsibility. If the formal norms can't be approved, bilateral dialogue is also helpful to formulate certain norms of behavior in a silent transforming way (LANG, 2015, p. 130).

The third one is a high-level path. It means that China and the U.S. can reach a broad consensus in cyberspace, formulating a mechanism of mutual recognition. The norms set by two countries can be promoted further to international norms which can be accepted by international society.

At present, China and the U.S. have not reached the above-mentioned low-level path. Although they have reached some agreements on providing information to each other for combating malicious cyber activity, anti-stealing cyber intellectual property and formulating national behavior norms in cyberspace, the two sides have a lot of misunderstandings on cybersecurity issues, especially on the basic concept of cybersecurity and cyber sovereignty. Therefore, on the initial stage of bilateral cyberspace norms' formulation, the negotiation process will still be in a low-level path. But on perspective of cyberspace's long-term development, the two sides' low-level negotiation process may leave a period of time for Chinese internet industry's development. It is necessary for China to accelerate domestic cyberspace governance experience. It can be seen that China's cybersecurity law and cybersecurity strategy were released in 2016. Through bilateral consultation, the two sides can standardize cyberspace in technic and legal aspects. Avoiding targeting or carrying out espionage on critical infrastructure provides prospects for China-U.S. negotiating a set of norms (Scott, Martin, & Astrid, 2016). In addition, China and the U.S. need to clear their bottom line on cybersecurity policies. The low-level and the middle-level path still play an active role in the global governance of cyberspace.

Negotiating Cyberspace Rule-Making in the Process of Participating in Global Cyberspace Governance

Apart from the bilateral dialogue on cyberspace norms' formulation, the multilateral global cyberspace governance also provides an essential platform for cyberspace rule-making negotiation. China and the U.S. should actively coordinate the global mechanisms for multilateral cyberspace governance, making full use of existing international organizations and multilateral mechanisms such as the UN, ICANN, International Telecommunication Union and World Internet Conference, so that every country can participate in consultation of the global cyberspace rule-making. China and the U.S. should play an important role in these multilateral negotiations, and take small countries' interests into accounts.

Promoting "Track Two Diplomacy" and "Track 1.5 Diplomacy" in the Field

The bilateral top or retired leaders, scholars, and enterprises' talk could also play an important role in cyberspace rule-making. Currently, China and the U.S. have formed the institution of track two diplomacy on cybersecurity. "Track two talks between China Institutes of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS)" is an important institution which started in 2009. China was staffed by CICIR; its delegations have included a growing number of government officials. U.S. was headed by CSIS but drew participants from across the Washington D.C., think-tank community, as well as an expanding cohort of government officials, to the point that it may be more accurate to view the dialogue as a Track 1.5, or mixed official-unofficial meeting (Scott et al., 2016).

Although the current diplomatic form has a strong official color, it has transformed into a stable mechanism, which is valuable in China-U.S. cybersecurity negotiation. In the long run, the two countries still need the semiofficial dialogue mechanism. Meanwhile, the official color of the mechanism may be reduced, attracting more think tanks and internet multinational corporations into dialogues to provide more recommendations. Besides, cyberspace rule-making interferes with many different fields including information technology, international relations, international law and so on, and it also relates to many interdisciplinary scholars. "Track Two and Track 1.5 Dialogue" can therefore benefit China-U.S. cyberspace rule-making.

Conclusion

With Chinese national power's rise and its internet industry's large development, China and U.S. will negotiate the issue more frequently. For China and the United States, the prospects of cyberspace rule-making in the future can be said that "the process is tortuous and the future is bright". If both sides accomplish the process of cyberspace rule-making, looking back on the process, they will regard it as an important event in the history of Sino-U.S. relations. The success of cyberspace rule-making not only benefits the bilateral relations, but also it plays an irreplaceable role in global cyberspace governance.

At present, the current cyberspace norms are dominated by the U.S. which takes the leading position in cyber issues. However, based on the large development, China has participated in cyberspace governance deeply. It is an important opportunity for China to show its national power and concepts. While enhancing mutual trust and outcomes of the consultations, China and the U.S. should make clear their respective strategic objectives and bottom lines in cyberspace. Only in this way can the consultation of the two countries on cyberspace rule-making go out of the low-level path and move towards the middle-level and high-level paths.

References

Cyberspace Administration of China (CAC). (2016). National Cyberspace Strategy. Retrieved from http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

DU, S. Z., WU, Y., & CHEN, Y. M. (2013, June 09). XI Jinping meets with President Obama. *People's Daily*.

DU, Y. Y. (2013). *The cognition of images on China by American government*. Beijing: Current Affairs Press.

Homeland Security. (2017). First U.S.-China law enforcement and cybersecurity dialogue. Retrieved from https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue

HUAN, L. (2016, January 09). To advocate the cyber sovereignty in a clear-cut manner. *Guangming Daily*.

LANG, P. (2015). Inter-state game in cyberspace governance. In S. M. Li, & Y. Y. Zhang (2015), *Annual report on international politics and security* (pp.). Beijing: Social Science Academic Press.

Michael, N. S. (2013). *Tallinn manual on international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Ministry of Foreign Affairs of the P.R.C. (2015). Full text: Outcome list of President XI Jinping's state visit to the United States. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1300771.shtml

Ministry of Industry and Information Technology of the P.R.C. (2016). Cybersecurity Law of the People's Republic of China. Retrieved from http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html

Ministry of Police. (2016). Taking top leaders' consensus into practice between China and the US. starting hotline mechanism of cybersecurity. *China Information Security, 1*, 17.

Robert, O. K., & Joseph, S. N. (2010). *Power and interdependence.* London: Longman.

Scott, W. H., Martin, C. L., & Astrid, C. (2016). Getting to Yes with China in cyberspace. Rand Corporation. Retrieved from http://www.rand.org/pubs/research_reports/RR1335.html

Stephen, K. (1982). Structural causes and regime consequences: Regimes as intervening variables. *International Organization, 36*(2), 185-205.

The Central People's Government of P.R.C. (2013). YANG Jiechi talks about President XI Jinping and President Obama Annenberg meeting achievements. Retrieved from http://www.gov.cn/ldhd/2013-06/09/content_2423489.htm

The White House. (2016). Fact sheet: Cybersecurity National Action Plan. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

United States Information Technology Office (USITO). (2016). China publishes first National Cyberspace Strategy. Retrieved from http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy

U.S. Department of Defense. (2015). Fact sheet: The Department of Deference (DoD) Cyber Strategy. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf

Xinhuanet. (2012). Full text of HU Jintao's report at 18th Party Congress. Retrieved from http://news.xinhuanet.com/english/special/18cpcnc/2012-11/17/c_131981259_12.htm

Zachary, G., & Jerome, A. C. (2016). Differing outlooks impede Sino-US cooperation to enhance cybersecurity. *South China Morning Post*. Retrieved from http://www.scmp.com/comment/insight-opinion/article/1846146/differing-outlooks-impede-sino-us-cooperation-enhance

ZHENG, Y. W., & HUANG, A. (2015). XI Jinping talk about the internet in four days, the issue of cybersecurity becomes highlight in his state visit in the US. *The Papers*. Retrieved from http://www.thepaper.cn/newsDetail_forward_1379925_1