RCGCG
网络空间国际治理研究中心
RESEARCH CENTER FOR GLOBAL
CYBERSPACE GOVERNANCE

STRATEGIC STABILITY IN CYBERSPACE:

A CHINESE VIEW

ZHOU HONGREN

RCGCG
网络空间国际治理研究中心
RESEARCH CENTER FOR GLOBAL
CYBERSPACE GOVERNANCE

The Research Center on Global Governance of Cyberspace is a think tank specialized on the topics of cybersecurity and global cyberspace governance. Its purpose is to explore the global cybersecurity landscape and national cybersecurity strategies, to promote cooperative dialog in cyberspace between all countries, and to jointly build global governance mechanisms for cyberspace, while providing policy solutions and advice for the Cyberspace Administration of China, the Ministry of Foreign Affairs and other related government departments.

To date, the Center has developed cooperations with various organizations, including the UNICRI Centre for Artificial Intelligence and Robotics, the UN Commission on Crime Prevention and Criminal Justice (CCPCJ), the Massachusetts Institute of Technology (MIT), the Carnegie Endowment for International Peace, the Center for Strategic and International Studies (CSIS), Russian Academy of Military Sciences, the University of Leiden in Netherlands, and others.

The Research Center on Global Governance of Cyberspace was founded in December 2018 in a joint effort by the Shanghai Institutes for International Studies, the PLA National Defense University, Fudan University, Nanjing University, Xiamen University, the Shanghai Academy of Social Sciences and others, with its secretariat located at the Shanghai Institutes for International Studies.

◀ Dr. Hongren Zhou

● Dr. Hongren Zhou was graduated from the Department of Automation, Beijing University of Aeronautics and Astronautics, in 1962, Beijing, P.R. of China, and received his Ph.D. degree in 1984 from the Department of Electrical Engineering, University of Minnesota, USA.

● Before joining the United Nations, Dr. Zhou worked for the Chinese Government as a commissioner of the State Planning Commission and the Executive Director General of the State Information Center. He was responsible for the development of economic information systems in the Government of China. In the meantime, he was a deputy to the 7th National People's Congress of China and an active member of the Foreign Affairs Committee of the National People's Congress, and concurrently, a professor and senior research fellow with a number of well-know universities and research institutes in China.

● With the well-known United Nations Department of Economic and Social Affairs, Dr. Zhou was a senior interregional adviser on Informatics and ICT for development from May 1990 to December 2002. Over the 12 years or more of working with the United Nations, he had been overlooking the development of ICT and its applications worldwide, providing advisory services to many developing countries and managing relevant technical cooperation projects of the United Nations. His areas of responsibility included both managerial and technical issues with respect to ICT and development, such as leadership, policies, development strategy and strategic plan, legislation, methodologies and implementation of information infrastructures and systems.

● Since the year of 2003, Dr. Zhou serves as the Executive Vice Chairman of the Advisory Committee for State Informatization. Concurrently, he was a member of the High-Level Advisory Group to the UN ICT Task Force. He has been the Dean of the School of Economics and Management, the Beijing University of Posts and Telecommunications, since 2008.

CONTENTS

Strategic Stability in Cyberspace: a Chinese View

Zhou Hongren

Abstract: As the strategic importance of cyber security increases, how to foster a stable cyber order compatible with the current international order is one of the most urgent issues for the international community. Global cyberspace governance and strategic cyber stability maintenance have thus become two emerging scientific fields in international studies. Generally, there are three states of stability in cyberspace: stable, delicately stable, and unstable. To promote the study of cyber order and enhance rational decision-making, it is necessary to adopt a cyclic perspective and fully explore the transition of cyberspace among the three states. Global cyberspace governance is mainly about managing the cycle of transition of cyberspace and designing robust institutions to prevent instability; in those institutions, international norms, rules, and laws will be made as essential guidance for cyber behavior of individual countries. As existing human knowledge and theoretical frameworks are the basis of studies on cyber strategic stability, it is imperative that effective dialogue and joint research among all international stake holders be conducted on issues of their common concern, which helps shape the strategic thinking and policy deliberation of individual countries on cyberspace and foster an international order that is conducive to cyber strategic stability.

Keywords: cyberspace, strategic stability, cyber security, international order, governance.

Zhou Hongren is the Executive Vice Chairman of the Advisory Committee for State Informatization, People’s Republic of China.
His mailing address is: No. 190 Chaoyangmen Inner Street, Beijing 100010, China.

As a global commons, cyberspace is fundamentally changing people's way of production, life and thinking. As civilization develops, cyberspace has already become an integral part of society, the study of which is of far-reaching significance. Meanwhile, global cyberspace governance and cyber strategic stability maintenance have become two emerging scientific fields in international studies.[1] Chinese scholars' active participation in related studies will contribute to the knowledge base and theoretical frameworks of the world. An international order conducive to cyber strategic stability can only be fostered through effective dialogue and joint studies among all international stake holders based on their shared interests and concerns, which, in turn, will shape individual countries' cyber strategies.

The Rise of Cyberspace

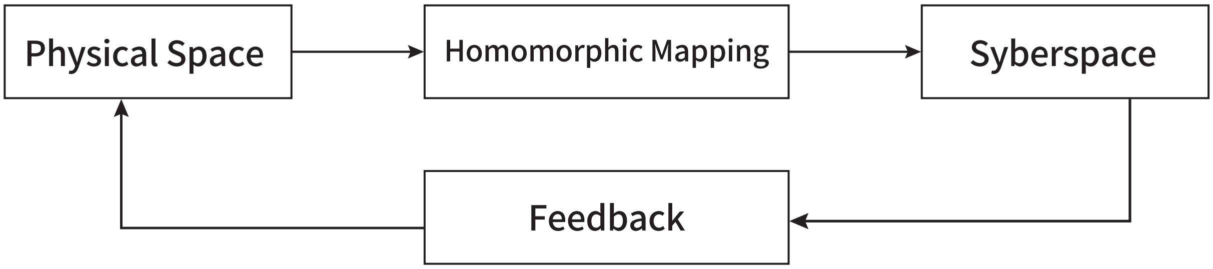
Cyberspace is the virtual space created by mankind. It not only overcomes the limitations of physical space in time and geography, but also transforms and integrates with the physical world through the development of science and technology. Cyberspace brings about new thinking and unprecedented possibilities in terms of technology, social institutions and civilization, while augmenting the difficulty of reaching consensuses across different fields and disciplines at the same time.[2] The U.S. Department of Defense defined cyberspace as the "fifth space," which is logically invalid. As a matter of fact, there exist only two realms: physical space and cyberspace. Land, air, sea and outer space are all physical space that can be mapped into cyberspace. Thus, in the study of cyberspace, it is necessary to first explore the concept, properties and evolution of cyberspace.

In social sciences, cyberspace is usually seen as the mapping of physical space into the digital world. In addition to related technologies, cyberspace also covers such dimensions in physical space as actors, behavior, as well as rules and norms, transcending the traditional "international norm dynamics."[3] To be more specific, political, economic, social, cultural, military, scientific and technological activities of mankind in physical space are mapped into cyberspace by the process of informatization. With the development of informatization, the mapping of physical space into cyberspace will be increasingly comprehensive and profound. This mapping is homomorphic rather than isomorphic; in other words, it is not one-to-one mapping.

(Highlight: *Human activities in physical space are mapped into cyberspace by informatization.)*

As cyberspace continuously expands and the data grow, cyberspace is affecting and controlling the operation of physical space in various forms (Figure 1). In modern society, mapping mainly relies on computers, information systems, and data communication networks, while feedback relies on big data, business intelligence, artificial intelligence and computational science. With the lasting development of information technology, cyberspace is growing ever larger and more complex; and more activities in physical space are mapped into cyberspace. Meanwhile, the use of data and information from cyberspace is also gradually transforming and improving physical space. In this sense, cyberspace is an instrument for mankind to comprehend and transform physical space.

Figure 1: Interaction between Cyberspace and Physical Space



(Source: Compiled by the author.)

As a result of technological advances, cyberspace has experienced three stages of development: the communication network, the information network, and the computing network; it is further merging with physical space, which has generated lasting -- sometimes subversive -- effect on technologies and their applications as well as society. As global informatization develops, more computer systems will be introduced into various physical systems and connected to the future global Internet of Things, thus acquiring different levels of intelligence. In this way, cyberspace and physical space are closely intertwined and exchange information through incessant homomorphic mapping and feedback, and will develop into one single, intelligent cyber-physical space eventually.

Cyberspace and Strategic Stability

As the strategic importance of cybersecurity increases, fostering a sustainable cyber order compatible with the current international order is a major challenge facing the international society. Cyber capabilities now constitute a vital part of national strength, and cyberspace has become a new arena for strategic competition among great powers. Naturally, cyberspace has become one of the priorities in global governance studies.[4] At present, the most critical issue facing cyberspace governance at the international level is maintaining strategic stability of cyberspace. For without basic stability, peaceful development of cyberspace will not be possible, which will threaten the strategic stability of physical space and ultimately harm peace and development of the world.

● Challenges to Strategic Stability in Cyberspace

The rising strategic position of cyberspace highlights the significance of establishing a reasonable cyber order. However, efforts of the international community in this regard have been hindered by strategic competition among major powers, a lack of governance mechanisms, and the "cyber security dilemma," endangering the peaceful development of cyberspace. In addition, as cyberspace and physical space are merging into cyber-physical space, strategic stability of cyberspace should also be conducive to, and reflected in, the stability of the international system and global nuclear strategic stability. Thus, three challenges must be tackled in promoting the strategic stability of cyberspace.

First is the weakening of the stability of the international system due to the subversive impact of cyberspace on physical space. Admittedly, the development of cyberspace has given rise to a new world order that undermines the stability of the existing international system, including the global security, economic, political, communications, technological and other regimes established after World War Ⅱ. But the international community -- national governments, enterprises, social organizations, and the like -- has yet to reach a basic consensus on the direction and impacts of such transition of international order. Hence, it is necessary to consolidate the stability of the international system while adapting it to the emergence of cyberspace.
*(**Highlight:** Joint efforts are needed to maintain stability of the international system while adapting it to the emerging cyberspace.)*

The second challenge is the influence of major-power competition on the stability of cyberspace during its rapid evolution. As cyberspace extends to more critical infrastructure in physical space -- such as energy, transportation, health, and finance -- that is closely related to the national economy and people's livelihood of individual countries, cyber security has become an ever graver concern of their national governments. [5] The strategic stability of cyberspace is not only vital to the national security of all countries, but it also plays an important role in shaping the order in cyberspace. Since cyber superpowers tend to adopt offensive cyber strategies, trying to strengthen cyber deterrence by "independent defense" and preemptive cyber strikes, mutual trust among them is lacking and a "cyber security dilemma" is taking shape, which undermines international cooperation both on cyber- and development-related issues. [6]

The third challenge is the potential damage of the integration of cyberspace and physical space to global nuclear strategic stability. Information technology can greatly improve the launch and early warning capability of nuclear weapons, but it can also increase the possibility of cyber attacks on the command-and-control systems of nuclear weapons. [7] Meanwhile, as cyber weapons are suitable for the first round of preemptive strikes to disrupt an opponent's perception of its actual situation, they are detrimental to maintaining the strategic stability between them and can easily lead to escalation of crises. Besides, traditional nuclear strategic stability is based on a clear understanding of the overall situation and smooth communication between opposing sides. Yet cyber attacks feature concealment and deception, which greatly harms the nuclear strategic stability between them.

● Choices for Strategic Stability in Cyberspace

Cyberspace is either stable, delicately stable, or unstable. During peacetime, stable cyberspace can be understood as a balance among major powers in cyber capabilities, conflict-management and governance mechanisms, as well as the security and development of their respective cyberspace. In other words, based on a balance of cyber capabilities among major powers, security and development of the cyberspace are hopeful to be achieved on the conflict-management and governance mechanisms. However, different from nuclear weapons, which can be measured by a variety of indicators to determine a country's national strength, assessing cyber weapons is extremely difficult, for they are programs based on codes, and as such, it is hard to measure their capabilities for destruction.

Although the United States is generally considered to be the strongest cyber power, evidenced by its Stuxnet attack on Iran's nuclear plant and the U.S. military's sizable investment in cyber warfare, the international community has not reached a consensus regarding the cyber capabilities of individual countries.[8] Especially in negotiations on reduction or control of cyber weapons, it would be difficult to quantify such capabilities, such as how to assess the cyber arsenal of a country, how to measure cyber weapons' attack capacity, as well as how to reduce and ensure the destruction of cyber weapons. These issues can hardly be resolved under the existing technological conditions and governance mechanisms, which poses enduring challenges to maintaining the strategic stability in cyberspace.
***(Highlight:** It is very difficult to quantify a country’s cyber capabilities.)*

Unstable cyberspace refers to a state of cyber war and conflicts. As there is no precedence of large-scale cyber warfare, the international community has not come to terms about what cyber warfare is and what impacts it may generate. Some scholars even argue that there will not be so-called "cyber war," because war will not happen in cyberspace alone, but cyber attacks will be combined with other means of attack in physical space. To avoid ambiguity, we can specify the three types of "unstable cyberspace": *(a)* conflict and war caused by cyber attacks on critical infrastructure in cyberspace; *(b)* conflict and war caused by cyber attacks aimed at destroying the command-and-control systems of strategic weapons, including nuclear and space weapons, etc.; and *(c)* massive instability caused by cyber attacks on economic, energy, communications, transportation, and other critical global infrastructure.

In comparison, delicately stable cyberspace refers to an intermediary state between stable and unstable cyberspace. Cyberspace today can be described as delicately stable, in which the overall balance and peace in cyberspace are maintained, but with constant cyber attacks, rising cyber arms race among major powers, and no global governance mechanisms on cybersecurity. [9] In this state, contingencies may easily escalate into acute crises, making the delicately stable cyberspace unstable. Fortunately, major powers have carried out cyber attacks with great caution, for they are still uncertain about the consequences of cyber conflicts and fear that cyber attacks may backfire on themselves due to spillover effect. For example, EternalBlue, a virus developed by the U.S. National Security Agency (NSA), was leaked by a hacker group and used as part of the WannaCry ransomware attack in 2017, endangering the U.S.' and global cyber security. Thus, in response to cyber threats, the United States tends to exercise deterrence and sanctions in other fields, such as economic sanctions and diplomatic measures, so as to prevent escalation of cyber conflicts.

To maintain stability in cyberspace, countries face important strategic choices. Cyber stability is better studied from a cyclic perspective, which also helps national governments make rational decisions. To be more specific, a country needs to adjust its cyber strategy to the three states of cyberspace: when cyberspace is stable but strategic competition with others continues, it might go all out to build its cyber defense system and enhance its cyber capabilities in case cyber war break out;

when cyberspace is delicately stable, it might be prepared to deal with low-intensity cyber conflicts and confrontation, and try to manage crises through negotiations and confidence-building measures, in case the crises escalate into war; once cyberspace becomes unstable, however, the goal of a country might have to be to win the potential war. In the meantime, a national government should frame appropriate international cooperation strategies to enhance global cyberspace governance, jointly exploring how to prevent war in stable cyberspace, how to reduce and control the damage caused by potential war in unstable cyberspace, and how to restore peace and order afterwards.

Key Technological Capabilities in Cyberspace

The main actors influencing cyberspace stability are national governments, whose behavior is determined by their key technological capabilities. There are four types of such capabilities that exert direct impacts on the strategic stability of cyberspace, including nuclear and space capabilities, strategic conventional armed forces, cyber capabilities, and capacity in emerging technologies. It can be said that the distribution of those key technological capabilities among countries determines the extent of strategic stability of cyberspace.

● Four Key Technological Capabilities

(1) nuclear and space capabilities have always been the most important strategic deterrents to any act that undermines global strategic stability, and thus have substantial impact on the stability of cyberspace.
(2) strategic conventional armed forces, including land, sea and air forces, can be used to destroy cyber infrastructure of an opponent,

such as network hubs, computer systems, and undersea cables.
(3) cyber capabilities can be used to undermine or even neutralize the previous two capabilities when the latter are highly dependent on cyber technologies. For instance, both the nuclear command-and-control system and the space communication system rely on cyber infrastructure, and thus are vulnerable to cyber attacks.
(4) capacity in emerging technologies, represented by artificial intelligence, can transform and upgrade the other three capabilities. Breakthroughs in the new technologies will fundamentally change the balance of power in the other three areas. For example, once quantum information technology is mature, it will develop much greater computing power and rewrite the current ways of encryption and decryption of information in communication, rendering unparalleled strategic advantages to those who possess the technology.

(Highlight:** Distribution of key technological capabilities among countries determines how stable cyberspace is**.)

● Distribution of Key Technological Capabilities

The distribution of the four key technological capabilities among countries is an important indicator in assessing the strategic stability of cyberspace. Drastic changes of any of them may disrupt the balance of global cyberspace.

As mentioned above, distribution of key technological capabilities among countries determines how stable cyberspace is. Like in the case of nuclear strategic stability where there is a balance among nuclear powers in their mutual destruction capacity and capabilities for second strikes, balanced distribution of strategic technological capabilities is most conducive to promoting the stability of cyberspace. For in this case, major powers would be very cautious about taking offensive actions and have much willingness to work with each other to establish the international regime for cyberspace governance. [10] In comparison, the absolute advantage or monopoly of a single country or group of countries over the strategic technological capabilities will lead to delicate stability of cyberspace. Today, the United States apparently dominates cyberspace with its supreme strategic technological capabilities. Such imbalance of distribution of strategic capabilities may further undermine the relative stability of cyberspace. For cyber technology is more accessible than nuclear technology; and it is relatively easy for national governments and even terrorist or organized criminal groups to acquire cyber weapons and launch cyber attacks. Therefore, in order to maintain strategic stability of cyberspace, it is of urgent importance for the international community to work together to prevent the proliferation of cyber weapons and cyber capabilities.

It should also be noted that the difficulty in assessing the key technological capabilities may cause great misjudgment of national governments, because the traditional means and institutions of measurement and verification in arms control do not naturally apply to cyberspace. First, it is difficult to assess cyber technologies, as they are usually virtual, dynamic and highly interactive. Second, it is hard to evaluate the cyber capabilities of countries for the general lack of transparency of related policies made by national governments; besides, national governments are constantly changing and adjusting themselves in building up cyber capabilities. Third, it is even more difficult to attribute cyber attacks to clear sources; and it is a common practice for national governments or other actors to evade punishment by denying any potential charge against them. [11]
(Highlight:** National governments tend to refrain from retaliating against cyber attacks by cyber means.**)

Moreover, it is not easy to judge the goal of a cyber attack, whether for warning, escalating a conflict, or retaliation. For example, after the Sony hack at the end of 2014, the U.S. government reportedly took measures to shut down the Internet system of North Korea. Yet it remains a mystery as to whether the United States actually took those retaliatory measures, or whether such retaliation was identified and recognized by the North Korean authorities. In most cases, the United States would launch sanctions in other areas in response to a cyber attack, including judicial prosecution, diplomatic pressure and economic sanctions, rather than retaliate directly by cyber means. However, such sanctions are not quite effective, because the absence of international regime on investigation and attribution of cyber offenses leaves a country vulnerable to the countervailing of the opponent.

Global governance for Strategic Stability in Cyberspace

To enhance global governance of cyberspace, it is necessary to develop robust institutions for better management of the transition cycle of strategic stability of cyberspace. The international regime on cyber governance should cover three levels: maintaining cyber security at the domestic level, such as safeguarding critical infrastructure; promoting cyber arms control and crisis management among major cyber powers; and enhancing common norms and laws at the international level.

Above all, national governments should take every effort to ensure the safety of the critical infrastructure of their countries, which is not only the basis of their national economy and people’s livelihood, but also important for maintaining strategic stability of cyberspace. The ability to safeguard their own critical infrastructure helps national governments to develop an objective and comprehensive perception of cyber security; only based on this can they make rational decisions and conduct sensible cyber behavior. On the contrary, the lack of such ability will create a strong sense of insecurity, which will increase the probability of miscalculation and crisis escalation, and prompt national governments to take radical actions. As vulnerabilities exist widely in the information systems of key industrial and business infrastructure, the protection of the infrastructure is both costly and difficult. For example, the U.S. government divides key U.S. infrastructure into 17 categories; to protect them costs considerable manpower, money, and material resources. Besides, many facilities of the key infrastructure are operated by private enterprises that have only limited resources and are often reluctant to disclose information about cyber attacks upon them. That makes cyber attacks easier whilst the anonymity of cyberspace increases the difficulty of proactive defense. [12]

Next, national governments, in particular those of major powers, must strengthen arms control and crisis management in cyberspace. Although cyberspace is different from physical space, the basic motivation of national governments -- to pursue their national interests -- remains the same. The “security dilemma in cyberspace” makes it very difficult for national governments to devote fully to arms control and crisis management in the field. For example, the dominant cyber power tends to dissuade other countries from developing cyber weapons, while the latter would strive to develop both offensive and defensive cyber weapons for self protection or as bargaining chips with the dominant power -- and this game goes on and on. Such arms race may be harmful to economic development of all countries. [13]

Notably, arms control in cyberspace does not provide the kind of reassurance as in the nuclear arms control in physical space. If the international community is certain that a national government has no plan to develop nuclear weapons, then it does not have to worry about a nuclear crisis, at least for the next few years. However, as most cyber weapons are intangible and many of them can be easily acquired from the global black market, cyber arms control has been extremely difficult. Similarly, crisis management is very difficult but crucial, too, for crisis outbursts in cyberspace are highly unpredictable. If a country is to carry out a cyber attack on another country, it tends to make covert preparations without producing any conclusive evidence about the attack. Once the attack is launched, a crisis may break out abruptly. In this context, how to respond to the crisis is crucial. As weapons of strategic deterrence, nuclear and space weapons must be under timely and effective management in time of crisis, since cyber attacks on nuclear and space facilities would destroy the past strategic balance of power, and are thus very likely to cause overreaction and escalation of conflicts.

(Highlight:** The international community needs to jointly formulate norms, rules and laws in cyberspace.**)

Furthermore, national governments should jointly formulate norms, rules and laws in cyberspace, for they are a collective expectation of responsible actors in cyberspace, which will contribute to the peace, stability, development and prosperity of cyberspace. [14] As emphasized in the 2015 report by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, common cyber norms are key to promoting the peaceful use of communication technologies as well as global social and economic development. It was also proposed in the report that national governments should not allow any internationally wrongful acts committed in their territories, and that they should respond appropriately to requests for assistance from other countries faced by cyber attacks on their critical infrastructure. [15]

Control and nonproliferation of cyber weapons should also be an integral part of cyber norms.[16] Should cyber warfare happen, nonproliferation of advanced cyber weapons would be crucial, since lasting cyber warfare may very likely end in acute conflicts in physical space. If cyber weapons are to be effectively controlled, the concept of weapons needs to be extended. The necessary conditions for cyber attacks include background knowledge of the target and its vulnerabilities. In general, it is very difficult to acquire such knowledge; but once a vulnerability is identified, there are many ways to weaponize the knowledge. In other words, the verification of cyber weapons is very difficult, and so is the control of them. Therefore, the international community must attach great importance to the control and nonproliferation of potential weapons in cyberspace.

Compared with cyber norms, international laws are legally binding and tends to have more effect on cyber behavior of countries. The 2015 report by the United Nations Group of Governmental Experts carefully examined how international laws applie to communications technologies and proposed that the basic principles of the Charter of the United Nations be applicable to cyberspace, including sovereignty, settling international disputes by peaceful means, and refraining from the threat or use of force against the territorial integrity or political independence of any state, and so on.[17]

However, there remain many disputes in the international community on the issue, especially with regard to the right to self defense in cyberspace, on which the Group of Governmental Experts, too, failed to reach a consensus. The U.S. representative insisted that national governments have the right to self-defense in cyberspace, while Russian representative Andrey Krutskikh stressed that Russia is “particularly concerned about the fact that the concept of forceful and military countermeasures in the digital field, which, among other things, implies the imposition of sanctions and punishment of ‘undesirable’ states bypassing the existing mechanisms, including the UN Security Council, is being imposed on the world."[18] Obviously, differences in understanding lead to different positions. Thus, it is of utmost importance for the international community to strengthen dialogue and negotiation, so as to foster the basic common understanding for rational strategic and policy deliberation of individual countries.

[1] Joseph Nye, "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance Paper Series, No. 1 (2014), pp. 5–13, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

[2] Chinese Ministry of Foreign Affairs and the State Internet Information Office, "The International Strategy of Cooperation on Cyberspace," March 1, 2017, http://www.catl.org.cn/2017-03/07/content_40498343.htm.

[3] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," International Organization, Vol. 52, No. 4 (Autumn 1998), pp. 887–917, https://home.gwu.edu/~finnemor/articles/1998_norms_io.pdf.

[4] John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," American Foreign Policy Interests, Vol. 36, No. 5 (2014), pp. 286–293.

[5] Brandon Valeriano and Ryan C. Maness, Cyber War Versus Cyber Realities: Cyber Conflict in the International System (London: Oxford University Press, 2015), pp. 20–23.

[6] Joseph Nye Jr., “Deterrence and Dissuasion in Cyberspace,” International Security, Vol. 41, No. 3 (2017), pp. 44–71.

[7] Robert Jervis, “Some Thoughts on Deterrence in the Cyber Era,” Journal of Information Warfare, Vol. 15, No. 2 (2016), pp. 66–73.

[8] Trey Herr and Drew Herrick, “Understanding Military Cyber Operation,” in Richard Harrison and Trey Herr, eds., Cyber Insecurity (Maryland: Rowman & Littlefield, 2016), p. 216.

[9] Martin Libicki, Cyber Deterrence and Cyberwar (Santa Monica: RAND Corporation, 2009).

[10] Madeline Carr, “Power Plays in Global Internet Governance,” Millennium: Journal of International Studies, Vol. 43, No. 2 (2015), pp. 640–659.

[11] See Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks, ” Journal of Strategic Studies, Vol. 38, No. 1–2 (2015), pp. 4–37.

[12] Lu Chuanying, “网络空间安全困境及治理机制构建 (Cyber Security Dilemma and Governance Mechanism),” Contemporary International Relations, Vol. 11 (2018), p. 50.

[13] Scott Warren and Martin Libicki, Getting to Yest With China in Cyberspace (California: RAND Corporation, 2016), p. 30.

[14] Karsten Geier, “Norms, Confidence and Capacity Building: Putting the UN Recommendations on Information and Communication Technologies in the Context of International Security into OSCE–Action,” European Cybersecurity Journal, Vol. 2, No. 1 (January, 2016).

[15] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly Document A/70/174, July 22, 2015.

[16] Kate Conger, “Microsoft Calls for Establishment of a Digital Geneva Convention,” Tech Crunch, February 14, 2017, https://techcrunch.com/2017/02/14/microsoft–calls–for–establishment–of–a–digital–geneva–convention/.

[17] Lu Chuanying, "新形势下如何进一步在联合国框架下加强国际网络安全治理 (How to Strengthen the International Governance of Cybersecurity under the Framework of the United Nations under the New Situation)," China Information Security, Vol. 2 (2018), p. 36.

[18] Andrey Krutskikh, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere," June 29, 2017, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.