Cyberspace Security: Trends, Conflicts and Strategic Stability

Xu Longdi

In recent years, conflicts and stability of cyberspace have become an increasingly major concern to many countries, who treat cyberspace as a strategic domain and have strengthened their cyber defense and offense capabilities. Cyberspace has been regarded as the "fifth domain," of equal strategic importance as the land, sea, air and space. This has intensified international competition in the field. This article will first outline the trends of cyberspace security, then examine the possible sources of cyber conflicts, and finally explore feasible solutions to maintain stability in cyberspace.

Trends of Cyberspace Security

China's National Cyberspace Security Strategy, released in December 2016, states that China faces seven opportunities and five challenges in cyberspace.[1] While it offers an official overview of the current security trends in cyberspace, this paper intends to elaborate from the perspectives of technological changes and innovation, cyber threats, competition among major powers, militarization of cyberspace, and cyberspace governance and rules-making.

Technological changes and innovation maintains strong momentum, while cyber threats are more complex and varied.

Continuous innovation of information and communications technology

Xu Longdi is Associate Research Fellow at China Institute of International Studies (CIIS).

1 "National Cyberspace Security Strategy," *Xinhua*, December 27, 2016, http://news.xinhuanet.com/2016-12/27/c_1120196479.htm.

(ICT) has been the key to the development of cyberspace. Without this, there is neither security nor risks in cyberspace. In recent years, many countries have been increasing their investment in information technology and cyber security, thus further promoting and accelerating technological changes and innovation. Now, big data, cloud computing and the internet of things are at the height of development, while artificial intelligence (AI) and smart cities are also booming. At the same time, trusted computing and quantum communications are taking the lead in a new round of technological development.

Technological progress has always been a double-edged sword. New information technologies bring not only progress and security but also risks and threats; and they can be grasped and exploited by both white-hat and black-hat hackers, as well as by criminals and terrorists. At present, cyber threats are becoming more and more sophisticated and are springing up one after another, ranging from personal information and privacy leaks to infringements of intellectual property, from cybercrimes and cyber terrorism to various sophisticated cyberattacks. For instance, according to the 2016 Tencent Internet Security Report, the threats and risks posed by malicious viruses, rogue software, Trojans and online fraud continued to rise in 2016.[2] The 2016 China Internet Security Report, released by 360 Internet Security Center, pointed out that advanced persistent threats (APT) have exerted significant and noteworthy impact in three areas: damage to industrial systems, cybercrimes against financial systems, as well as geopolitics.[3] The recent WannaCry ransomware attack and related EternalBlue exploit once again highlighted the complexity, variability, and seriousness of cyber threats.

Competition among great powers continues to rise as they scramble to seize the commanding height of cyberspace.

In recent years, many countries have introduced cyber security policies

2 "Tencent Internet Security Report 2016," January 20, 2017, http://slab.qq.com/news/authority/1545.html.

3 "China Internet Security Report 2016," February 15, 2017, http://zt.360.cn/1101061855.php?dtid=1101062514&did=490278985.

and strategies, established relevant institutions, recruited professional talents, strengthened cyber legislation and law enforcement, and carried out international cooperation. As a result, cyber relations are becoming a new dimension of international relations as cyberspace is becoming a new domain for competition among great powers.

International relations in the real world are also reflected in cyberspace. For instance, countries such China and Russia unequivocally support the principle of cyber sovereignty, while Western countries such as the United States and the United Kingdom vigorously advocate the idea of cyber freedom. Former US secretary of state Hillary Clinton spared no effort in conducting cyber diplomacy and promoting cyber freedom. In practice, the United States have attached great importance to forwarding its diplomatic messages with various information platforms, among which social media has become a new tool of American diplomacy. Although the US expects to occupy the international moral high ground through cyber diplomacy, many developing countries fear that freedom in cyberspace is just another pretext for the West to meddle in their internal affairs and violate their sovereignty, and worry that the West is seeking to engage in "color revolutions" through cyber means so as to undermine their national security, stability and development.

Cyber sovereignty is a natural extension of national sovereignty in cyberspace. After years of continuous negotiations, especially the persistent efforts of the United Nations Group of Governmental Experts (UNGGE) on information security, the principle of cyber sovereignty has been recognized by such international organizations as the United Nations and NATO[4] and countries such as the United States,[5] thus laying the foundation for future global internet governance and cyber strategic stability. However, the meaning of cyber sovereignty is still disputed. Of course, both cyber freedom and cyber sovereignty are relative in their significance and cannot be pushed to the extreme; otherwise,

---

4 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

5 Harold Hongju Koh, "International Law in Cyberspace," September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm.

Locked Shields 2017, the largest and most advanced cyber defense exercise in the world, was launched in Tallinn, Estonia on April 26, 2017. The exercise involves around 800 security experts, policy officers and legal advisors from 25 NATO allies and partners.

these abstract principles may become a hindrance for a country's internet development. For example, the European Union attaches so much importance to such values as human rights, democracy and privacy in its cyber policy that its internet development lags far behind that of the United States.

With regard to internet governance, countries such as China and Russia support the multilateral approach with governments taking a leading role, while the United States and other Western countries advocate a multi-stakeholder approach in which multiple actors participate, thus diluting the role of governments. The latter maintains that internet governance should take a bottom-up approach, in which actors like technical communities, individuals, and internet companies play a leading role, while governments are only one of the stakeholders. This is in line with the historical experience of the internet's rise in the United States, but it runs against the fact that the US government once lent vigorous support for the development of the computer network. Therefore, the United States considers more of its expedient

needs but ignores the historical facts in its advocacy and support for the multi-stakeholder approach to internet governance. In contrast, the multilateral approach is more in line with the national conditions of China, Russia and developing countries whose primary task is to strive for IT development. In this process, there is no doubt that their governments play a greater role in planning, guiding and coordinating the development of cyberspace, while neither the market nor the bottom-up social forces can accomplish it. This is still true of numerous less developed countries today. Of course, along with the rapid expansion of the internet and the gradual growth of technological capabilities, it has become a "strategic necessity" for the participation of multiple actors in internet governance, as the government alone is not able to achieve effective cyber security. In fact, a one-dimensional approach is insufficient for either global or domestic internet governance, which instead needs a multi-dimensional approach, covering multiple actors, a multi-layered governance structure and multiple issues. Thus, both the multilateral approach and the multi-stakeholder approach constitute an integral part of any internet governance model.[6]

Cyber power is a foundation of international competition and incorporates such elements as technology, personnel, economy, military and culture. The revelations by the whistle-blower Edward Snowden have offered the world a glimpse of the leading edge of the United States' cyber power. The cyberattacks on Estonia, Georgia and Ukraine, widely reported by Western media, might be traces of Russian cyber power. Now, four of the world's top 10 internet companies, Alibaba, Tencent, Baidu and JD, come from China, which might highlight the power of China's internet economy. However, cyber power, just like national power, has also been in flux. In recent years, many countries have increased their investment in order to participate in the fierce cyber competition, even the United States, which enjoys extraordinary advantages in cyber power,

6 China states in its International Strategy of Cooperation on Cyberspace, released on March 1, 2017, that "China calls for enhanced communication and cooperation among all stakeholders including governments, international organizations, Internet companies, technological communities, non-governmental institutions and citizens. Relevant efforts should reflect broad participation, sound management and democratic decision-making, with all stakeholders contributing in their share based on their capacity and governments taking the leading in Internet governance particularly public policies and security." See "International Strategy of Cooperation on Cyberspace," *Xinhua*, March 1, 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

is no exception. Japan, Australia and other countries are also making great endeavors to build their cyber capacities. Of course, for less developed countries, internet development and narrowing the digital gap remain their top priority.

Cyberspace is marching toward vigorous militarization.

The existence of a cyber war is still controversial in theory, but there is no doubt that in practice ICT can be used for war. In recent years, the militarization of cyberspace has become more and more prominent, which is reflected in the flourishing ideas and theories on cyber war, the growth of cyber forces, and the research and development of cyber weapons, thus adding a new area of competition among nation states.

In the mid-1990s, the RAND Corporation put forward the idea of "strategic information warfare"[7] and held that a "cyber war is coming."[8] Over a decade later, William J. Lynn III, then US. Deputy Secretary of Defense, wrote, "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as the land, sea, air, and space."[9] In December 2012, then US Defense Secretary Leon Panetta said that the US Department of Defense had drafted new rules of engagement in cyberspace, which would enable the US military to respond more quickly to cyber threats. Russia has also conducted extensive theoretical research on cyber warfare from an early stage. The Information Security Doctrine of the Russian Federation, adopted by Russian Information Security Committee in 2002, listed cyber war as a sixth-generation war and charted the course for the development of Russian cyber forces. In short, Russia has attached great importance to cyber war, in particular the command of the information and electromagnetic domain. At its Warsaw Summit in July 2016, NATO recognized cyberspace as a "domain of operations" in which it would defend itself as it does in the air, on land, and at

---

7 Roger C. Molander, et al., *Strategic Information Warfare: A New Face of War*, RAND, 1996.

8 John Arquilla and David Ronfeldt, "Cyberwar is Coming!" in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflicts in the Information Age*, RAND, 1997, pp.23-54.

9 William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5, September/October 2010, p.101.

sea, and would focus on improving the cyber capabilities of its member states.[10]

Many countries have begun to build their cyber forces and related structures in an attempt to seize the initiative in cyber offense and defense. In June 2009, the United States set up a Cyber Command subordinate to the Strategic Command, conferring the new mission on its military of seeking dominance in cyberspace. On August 18, 2017, the United States elevated its Cyber Command to the status of Unified Combatant Command focused on cyberspace operations, whose head would report directly to the Secretary of Defense.[11] A US Cyber Command news release said, "All 133 of the US Cyber Command's Cyber Mission Force teams achieved initial operating capability as of October 12, 2016."[12] The Russian armed forces have also established "information forces" that are responsible for offense and defense in information warfare, with a view to ensure an advantageous position in information confrontation. The United Kingdom, South Korea, Japan, India and other countries have also set up their own cyber forces.

Countries have also been increasing their investment in the R&D of cyber weapons. The United States is well ahead of the rest of the world in this regard. In 2008, the Pentagon spent $30 billion building the National Cyber Range comparable to the Manhattan Project. In 2012, the Pentagon's budget for cyber security and information technology reached $3.4 billion. The Pentagon has also developed a list of cyber weapons and cyber tools, whose use is broken into three tiers: global, regional and area of hostility, thus providing a foundation for waging cyber warfare in the future.[13] Moreover, countries are also making great efforts to

---

10 "Warsaw Summit Communiqué," Press Release (2016) 100, July 9, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en.

11 The White House, "Statement by President Donald J. Trump on the Elevation of Cyber Command," August 18, 2017, https://www.whitehouse.gov/the-press-office/2017/08/18/statement-donald-j-trump-elevation-cyber-command; Munish Sharma, "US Ups the Ante in Cyberspace," August 26, 2017, http://www.eurasiareview.com/26082017-us-ups-the-ante-in-cyberspace-analysis.

12 "Initial operating capability" means that all Cyber Mission Force units have reached a threshold level of initial operating capacity and can execute their fundamental mission. See Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability," October 24, 2016, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability.

13 Ellen Nakashima, "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare," *The Washington Post*, May 31, 2011, https://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html?utm_term=.7fb8069678ec.

train their cyber forces. In short, despite the absence of a cyber war that leads to large-scale human casualties, countries are now scrambling to prepare for cyber warfare, and cyberspace is being increasingly militarized and weaponized. In other words, a cyber arms race has quietly begun.

Cyberspace governance, in particular cyber rules-making, move from principles to action.

After years of arduous bargaining among multiple actors, the macro-structure of global cyberspace governance seems to be on the horizon. Just like global governance in other areas, rules are also at the heart of global cyberspace governance. Cyber rules can be divided into two levels: general rules (abstract principles) and specific rules on a concrete subject matter. The international community, especially the United Nations Group of Governmental Experts on information security, has reached important consensus on such general rules as cyber sovereignty and cyber freedom, and acknowledged that international law, and in particular the Charter of the United Nations, is applicable to cyberspace.[14] In the future, all parties should go beyond general rules and abstract principles and move toward specific and concrete rules that are of pragmatic value. Of course, there are different types of cyber rules dealing with diverse cyber threats, such as cybercrimes, cyber terrorism, cyber warfare, data leakage (privacy protection), and technological vulnerabilities (technical standards).

The vast majority of cyberattacks fall into the category of cybercrimes, which remain the biggest cyber threat, but now there are not yet universal international treaties or laws to address cybercrimes. Terrorists and terrorist organizations are increasingly using the internet to disseminate audio and video programs that incite violence, spread terrorist and extremist ideologies, recruit followers, raise money, and plan and carry out terrorist activities. The threat of cyber terrorism is not negligible. In 2016, the United States announced that it would launch

14 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/68/98, June 24, 2013, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement; "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

cyberattacks against the Islamic State group. Some scholars think that "cyber war is coming," while others insist that a "cyber war will not take place."[15] However, the increasing militarization of cyberspace is an indisputable fact. Therefore, how to regulate a country's behavior in cyberspace, especially military behavior, should be a focus of future work for all parties. Technical elites are discovering and creating numerous vulnerabilities and loopholes on a daily basis, and large-scale data leaks were the most prominent cyber threat in 2016. Accordingly, technical standards should be another focus of future cyberspace governance.

In the years ahead, the international community needs to decide on specific rules to deal with different cyber threats, and strive to surpass the "abstract" period and move towards a "concrete" era. In this regard, the big powers, the United States and China included, should engage in constructive dialogue and cooperation, make cyberspace governance not descend into empty talk, and leave no room in which terrorists and criminals can maneuver.

Cyber Conflicts and Strategic Stability

The abovementioned security trends in cyberspace indicates that cyberspace is faced with unstable factors, which has brought the issue of cyber strategic stability to the fore. Strategic stability originally referred to the strategic posture of mutually assured destruction through nuclear deterrence of the United States and the Soviet Union during the Cold War. Recently, it has been applied to elaborate on the strategic posture of cyberspace.

Cyber strategic stability refers to four things: (1) well-functioning ICT systems; (2) countries keeping normal, stable and peaceful state-to-state relations in cyberspace, rather than being caught in cyber conflicts and confrontation; (3) inter-state military conflicts do not lead to chaos in or paralysis of cyberspace, or to put it simply, there will not be a state of "cyber war"; (4) peaceful use of cyberspace for human, economic, and social purposes. On the whole, cyber competition and conflicts among states are most likely to cause strategic

15 Thomas Rid, *Cyber War Will Not Take Place*, London: Hurst & Company, 2013.

instability in cyberspace. Therefore, this section will explore the possible sources of cyber strategic instability from the perspective of international relations.

Typology of cyber conflicts

Cyber conflicts can be divided into linguistic conflicts, ideational conflicts, conflicts of interests, and military conflicts. Of course, cyber conflicts can sometimes be taken for cyber differences, cyber disputes or cyber disagreements, which are also important factors contributing to cyber instability.

Linguistic conflicts. Language differences are in fact still the biggest obstacle to agreement in the virtual world. For example, there are such expressions and terms as cyber, cyberspace, internet, and networks in the English language. Nevertheless, when translating them into other languages, we might encounter some difficulties, which are sometimes troublesome as it can be hard to find a direct equivalent in the target language. In Chinese academic circles, there are even disputes over transliteration (*Yin Te Wang*) and free translation (*Hu Lian Wang*) of the term "internet." In addition, the United States and other Western countries usually use the term "cyber security," while Russia uses "information security." China used to employ "information security," but now uses both terms. So far, this situation has not caused too much trouble in international exchanges, but the differences between disparate parties do exist and constitute one of the sources of cyber conflicts.

To some extent, what Western scholars called "fragmentation" of cyberspace is also a result of language differences. When accessing the internet, most internet users will use their native language to browse news websites, do shopping online, and so on. In this sense, language differences have caused the real fragmentation of cyberspace. However, the accusations made by Western countries that other countries are "fragmenting" cyberspace are not well-founded, as even if a country tries to build an area network it is inseparable from the global internet infrastructure and its schema, and thus it remains part of the global internet.

Ideational conflicts. As mentioned earlier, countries have explicit divergences over cyber sovereignty and cyber freedom. This phenomenon has

a close link to the ideational and ideological conflicts between states in the real world. On many occasions, when countries are talking about cyber sovereignty, they often mean different things with the same term. The West focuses more on the control of cyberspace and the right of citizens to access the internet, while developing countries like China place more emphasis on the right to development, the right to administrative jurisdiction, and the right to and not to engage in international cooperation in cyberspace. Chinese President Xi Jinping, in his speech at the Second World Internet Conference held in December 2015 in China's eastern town of Wuzhen, advocated the principle of respecting cyber sovereignty when promoting reform of the global internet governance. He said, "We should respect the rights of individual countries in choosing their own internet development path, internet governance, and internet policies and take part in cyberspace governance on an equal basis, and not push cyberspace hegemony or interfere in other countries' internal affairs or engage in or support cyberspace activities that jeopardize the national security of others."[16] This has been the most explicit statement of China's position on cyber sovereignty to date.

There are also cognitive divergences over cyber freedom, cyber privacy, cybercrime, cyber espionage, and cyber terrorism among different countries and peoples. For instance, some think that all personal information is privacy and should be respected and protected, while others deem that only sensitive personal information pertains to privacy. Similarly, due to differences in history, culture, religion and tradition, what constitutes a crime in one country is not necessarily a crime in another. Thus, when countries negotiate and communicate over the abovementioned issues, some conflicts might occur.

Conflict of interests. Just as in the real world, different countries are also at different levels of ICT development, face different historical tasks, pursue different strategic goals, and enjoy different interests in cyberspace. Such divergences over interests are a significant factor for cyber conflicts. For example, the primary goal of numerous developing countries, including China, in cyberspace is to develop ICT, build information infrastructure,

16 "Xi Calls for Respect for 'Internet Sovereignty'," December 16, 2015, http://www.wuzhenwic.org/2015-12/16/c_47570.htm.

enhance cyber power, and safeguard cyberspace security. Therefore, they attach greater importance to cyber sovereignty in order to defend their right to cyber development, jurisdiction over their networks and international cooperation. In contrast, the United States enjoys huge cyber superiority, seeks to gain dominance in cyberspace, and pursues absolute cyber security. However, as the Snowden revelations demonstrate, many of the United States' practices and behavior when pursuing its own national interests or defending its superior status in cyberspace have posed serious threats to other countries' cyber security, thus proving to be an important cause of cyber instability.

Moreover, for the sake of promoting such values as human rights, democracy and freedom, the United States and other Western countries employ information technology and social media to interfere in other countries' internal affairs, usually leading to political unrest and instability. In addition, the US has repeatedly accused Chinese hackers of stealing US intellectual property and of damaging US business interests. On those grounds, the US even indicted five Chinese servicemen for cyber espionage in 2014. However, in theory, the legal status of espionage in international law is very complex; it is not simply prohibited. In short, disparate cyber interests have become a crucial reason and even excuse for cyber conflicts, which are easy to spill over into the real world, thus not only threatening the strategic stability of cyberspace, but also harming normal interstate relations.

Military conflicts and cyber warfare

There are various types of cyber activities, whose nature varies, as does people's perception of them. Cyber warfare is the most extreme cyber activity and cyber conflict. On the whole, there is still no consensus on the existence of cyber warfare. As mentioned earlier, one school of thought maintains that cyber warfare exists and has already occurred, while another school of thought contends that cyber warfare does not exist and will not take place.

Attackers and targets. In general, there are three levels of cyberattacks, namely those by individuals, those by groups and those by states. They can be configured in six pairs as individual-individual, individual-group, individual-

state, group-group, group-state and state-state. In terms of these configurations, it is only state-state attacks that can be called acts of war, whereas it would be hard to describe attacks among the other five pairs in this way. Of course, if an individual or group is authorized or instructed by a state, this could also constitute an act of war. However, because of the unique nature of cyberspace per se, it is difficult to attribute an attack. Therefore, it would be hard to identify the attacker and to infer whether cyber warfare exists or not.

In terms of attackers' targets, they often include: computer operating systems and software or hardware; soft resources and computer information such as personal information, corporate secrets and intellectual property; and critical infrastructure such as banking systems, airlines, communications, dams and power stations. These targets might be individual, group or state assets, being at different levels and of different value. Therefore, it would be very difficult to determine the existence of cyber warfare from just one factor or criterion. This is also a Gordian knot in defining cyber warfare from the perspective of attacker or target.

Objectives and consequences. Just as with the different types of cyber activities, there is a huge variety of objectives for cyberattacks. Some attacks are purely borne out of the attackers' interest and curiosity, or to demonstrate their computer talents and abilities. In fact, a majority of early hacking falls into this category. Some attacks are to gather corporate secrets, gain economic advantages or perpetrate online fraud. Some are for sabotage, including deleting information from a target computer, paralyzing the target computer's software and operating system, or damaging the computer's hardware or information infrastructure. Of course, some cyberattacks might be used for war purposes.

Accordingly, attacks with different objectives will also bring about disparate consequences, including loss of personal and commercial information, theft of intellectual property rights, sabotage of computer hardware and software, corruption of a computer's operating system, destruction of key information infrastructure or even human casualties. Apart from human casualties, all of these other consequences have occurred, but it is very difficult to see them as constituting cyber warfare. Even if attacks result in casualties, these still have to

be differentiated according to whether they were caused directly or indirectly. All these factors would influence the decision as to whether cyber warfare has already taken place or whether it even exists.[17]

Therefore, when analyzing and evaluating the nature of cyber incidents, one must take an overview of the abovementioned factors in a comprehensive manner. One must make an objective analysis of a specific situation, including the attacker and victim of the attack, the objectives, as well as possible consequences. We should not exaggerate or overlook facts, and should avoid oversimplifying cyber warfare by lumping all cyberattacks together under the rubric of "acts of war." Ultimately, it might be up to the highest political leadership to decide whether there is an occurrence or existence of cyber warfare. Therefore, it is a political decision and political behavior. Furthermore, if the attack is attributed without doubt, the intention clear, the consequences extremely serious, and the political leadership can determine the existence and occurrence of cyber warfare in the end, then the strategic stability of cyberspace has been broken. Or, when two countries are in a state of conventional war, for which cyberspace is only one of the tools available to both of the warring states, there would not be cyber strategic stability to speak of; instead, it would have entered the realm of war operations. In short, cyber warfare is an essential disruption of the strategic stability of cyberspace.

Shaping Cyber Strategic Stability

Given the abovementioned cyberspace security trends and possible sources of cyber conflicts, the following section will explore feasible solutions to cyber conflicts, so as to better shape cyber strategic stability and maintain order, peace, and security in cyberspace.

Enhancing international exchanges and cooperation

Given the aforementioned types of cyber conflicts that might stem from

17 Xu Longdi, "The Applicability of the Laws of War in Cyberspace: Exploration and Contention," *Contemporary World*, No.2, 2014, pp.50-51.

the ideational and ideological differences among states, mutual exchanges and cooperation could be conducive to narrowing differences, forming consensus, and eliminating the root causes of cyber conflicts, thus further shaping and building the strategic stability of cyberspace, even though the divergences might not be removed completely.

In terms of linguistic conflicts, international exchanges could help forge consensus in a gradual manner and form a universal language that all parties agree on, understand and utilize. In fact, some pure technical language may be less controversial, while those terminologies with social and political implications may entail different interpretations in different circumstances, and are more likely to cause confusion and misunderstanding. In this regard, all parties should communicate with each other to reduce potential and unnecessary differences. China and the United States, and Russia and the United States have made some endeavors in this direction.

As for ideational conflicts, more exchanges could enhance mutual understanding and increase political trust, and freeze, shelve or dilute such fundamental divergences, thus avoiding conflict escalation and maintaining normal relations among states in cyberspace.

As far as conflicts of interests are concerned, on the one hand, countries should respect the interests of other countries while safeguarding their own, and should not do things harmful to others in cyberspace; on the other hand, countries could gradually cultivate and expand their common interests through cooperation, reduce the scope of their conflicts of interests, and defend their common security interests in cyberspace. China and the US, and Russia and the US have established hotlines on cyber issues, which are of great significance to increase mutual trust, dispel misunderstanding, resolve disputes and maintain robust cyber relations between them.

Building cyber power

As mentioned earlier, cyber power is the foundation of international competition in cyberspace. However, the cultivation and building of cyber power needs to be reflected in national strategic planning, and be

implemented in cyberspace strategic planning as well as in concrete R&D programs. In recent years, while Western developed countries have paid much attention to building and investing in their cyber power, various developing countries are catching up by making strategic plans and establishing relevant institutions. In this regard, China is no exception. China has not only put forward the strategic goal of building itself into a cyber power, but also set up a specialized agency, the Cyberspace Administration of China, to coordinate the work on cyber security. It has also introduced a series of policy papers, laws and strategic plans including the Cyber Security Law, National Cyberspace Security Strategy, International Strategy of Cooperation on Cyberspace, the 13th Five-year Plan on National Informatization, and other sectoral designs, laws and regulations.

Regardless of the content and strength of its cyber power, a country should have some core or key technologies and possess some offensive and defensive capabilities, and even deterrence capabilities, in order to maintain its cyber security and strategic stability. With advanced core technologies, a country might not necessarily be able to preserve cyberspace security. However, without them, no matter how perfect its top-level design is, no matter how strong its cyber security awareness is, and no matter how excellent its cyber culture is, there will not be cyberspace security to speak of for a country. Therefore, promoting technological innovation will be a primary task for many countries in a long period of time.[18]

Fostering cyber deterrence

Cyber deterrence might not be an effective solution to cyber conflicts, but it could help shape the strategic stability of cyberspace. Given the uniqueness of cyberspace, including the difficulty in attribution and diversity of actors, there is still a debate over the utility of cyber deterrence. Recently, Joseph Nye proposed that the effectiveness of cyber deterrence depends on

---

18 Xu Longdi, "Development, Security and Governance: An Agenda for China Cyberspace Governance," in Xu Jian, *Civilizational Revitalization and Remaking: Period of Strategic Opportunities in a Historical Perspective*, Beijing: People's Publishing House, 2016, p.388.

the answers not just to the question "how" but also to the questions "who" and "what." He also proposed four major mechanisms to reduce and prevent adverse actions in cyberspace: threat of punishment, denial by defense, entanglement, and normative taboos.[19] In other words, cyber deterrence could play a positive role in maintaining the strategic stability of cyberspace, although the functioning mechanisms might be different from those in traditional deterrence theories.

In terms of military conflicts or cyber warfare, cyber deterrence could also play a certain role, and even prevent the occurrence of cyber warfare, thus promoting the strategic stability of cyberspace. Moreover, we should also understand and solve cyber military conflicts within the framework of international relations, as cyber relations are a part of them. In this regard, building more stable and reliable state-to-state relations should be a focus. Therefore, in order to maintain a normal and good interstate cyber relationship, countries should exercise self-restraint in using cyber tools, and refrain from offensive actions, let alone preemptive strikes. In the meantime, as for the cyberattacks that they suffer from, countries should identify their real nature and respond cautiously. On regional and global levels, countries should conduct multilateral dialogues, manage and control potential military conflicts, and engage in cyber arms control to reduce the likelihood of escalating cyber conflicts.

In addition to the above proposals, other policy options are also available, such as promoting confidence-building measures, building international norms, and conducting cyber diplomacy. There might not be a causal relationship between these options and cyber conflict and cyber strategic stability, but in the long run, the former will contribute to the latter in a direct or indirect manner. In short, the international community should adopt a multi-pronged approach and take various measures to resolve cyber conflicts. Only in this way can we maintain the strategic stability of cyberspace and establish a peaceful, secure, stable and orderly cyberspace.

19 Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol.41, No.3, Winter 2016/2017, pp.44-71.