Cyber War Preparedness, Cyberspace Arms Control and the United States
About CIIS

China Institute of International Studies (CIIS) is the think tank of Chinese Foreign Ministry. Founded in 1956, CIIS is one of the oldest research institutions specialized in international studies in China. It conducts research and analysis focusing primarily on medium- and long-term policy issues of strategic importance to China, particularly those concerning international politics and world economy. It also makes comments and policy recommendations on major world events and hot-spot issues.

About CIIS Report

Contributed by researchers from CIIS and published aperiodically, CIIS Report brings forth a series of research papers on hot issues of international relations as well as on major aspects of China’s diplomacy. Presented with clear-cut views based on detailed and substantive information and in-depth analysis, CIIS Report aims at offering a comprehensive picture of assessment of the situation, academic studies and policy evaluation in clear and precise language. CIIS Report is published both in Chinese and English and downloadable on the website of CIIS (http://www.ciis.org.cn). The views expressed in CIIS Report are those of the author(s) or their research group only and do not necessarily reflect the official position of CIIS.
Cyber War Preparedness, Cyberspace Arms Control and the United States

Teng Jianqun
Xu Longdi

No. 3 - August 2014
SUMMARY

I. Introduction

II. Cyberspace and War
   A. The extension of war to cyberspace
   B. Controversy over the existence of “cyber-warfare”

III. Cyberspace and Arms Race
   A. Frequent occurrence of quasi-cyber war
   B. The increasingly intensifying arms race in cyberspace
   C. Preparations of the United States for cyber-warfare
      1. Formulating policies for cyber-warfare
      2. Setting up institutions and mechanisms
      3. Developing cyber-warfare capabilities
      4. Providing financial support

IV. The United States and Cyberspace Arms Control
   A. The attitude of the United States toward cyberspace arms control
      1. Two ways to regulate cyber conflicts and cyber-warfare
      2. The U.S. attitude toward cyberspace arms control
   B. The struggle for rule-making power in cyberspace arms control
      1. Competing cybersecurity policies
      2. Different types of cybersecurity rules
   C. Cyber-warfare and the rules for cyberspace arms control
      1. Cyber-warfare and the international treaty
      2. Cyber-warfare and the principles of armed conflict
      3. “Preemptive” cyberstrike policy goes against the trend

V. Cyberspace Arms Control and Sino-American Cyber Relations
   A. The development of the Internet and cybersecurity situations in China
   B. Viewing cyberspace arms control from the angle of Sino-American cyber relations
1. Setting up priorities for cyberspace arms control and focusing on regulation of state-sponsored online behaviors ................................................................. 48
2. The United States intends to dominate cyberspace arms control and China should actively participate in the process ................................................................................. 49
3. The United States has a relatively well-developed legal system on cyber issues and China can draw on its experience ........................................................................................................ 49
4. China and the United States should cooperate in exploring possible plans for cyberspace arms control .......................................................... 51
5. Promoting multilateral cooperation and global internet governance ..................................................................................................................... 53

Conclusion .................................................................................................................................................................................................................. 55
SUMMARY

Cyberspace has become an indispensable part of a state, a society and the life of individuals due to the rapid development and extensive application of information technology. Together with its convenience, cyberspace has also posed an increasing number of potential risks and challenges. To seek superiority in cyberspace, many advanced countries in information and communications technology (ICT) have formulated cyberspace policies and strategies. Preparations for cyber-warfare have become an important part of army building in quite a few countries. Besides nation-states, non-state actors have also taken advantage of the vulnerability and interconnectivity of the cyberspace to inflict enormous damage to countries and societies.

The cyber-attacks that Estonia, Georgia and Iran suffered as well as the U.S. PRISM spying scandal exposed in 2013 have demonstrated that there is increasing difficulty in maintaining order and security in cyberspace. However, despite preparations for cyber-warfare by various countries and cyber-intrusions by individuals, there is still a lack of international laws governing cyberspace, especially the law for cyberspace arms control. Since some countries enjoy an advantaged position in information technology, they are also unwilling to talk about restraints on cyber activities. Against such a backdrop, it has become an urgent necessity to formulate international rules and improve the international law system in order to counter cyber threats, maintain order and security in cyberspace, and regulate cyber activities. Cyberspace arms control has also become an important part of the international arms control and disarmament.

Since the 1970s, the United States has always been a leading country in information technology. By drawing on its advantaged position in information technol-
ogy and sufficient funding, it has worked out a relatively complete set of policies and strategies for cyberspace and is accelerating its pace in building cyber forces and carrying out theoretical research on cyber-warfare. As one of the major creators of the international order after World War II, the United States plays an irreplaceable role in international arms control and disarmament. Every single measure and action it takes in cyberspace will inevitably have a bearing on the development of international cyberspace arms control in the future.

This report presents first of all the general situation of current cyberspace, and then it introduces discussions on cyber-warfare in the international community and the restraints on cyber-warfare imposed by the existing international law as well as other issues. Subsequently, it analyzes cyber war preparedness and demands for cybersecurity of the United States and other countries. Finally, it proposes that a new regime and a new set of rules for cyberspace arms control be established so as to avoid the abuse of cyberspace and not to trigger international conflicts, for which the United States has unshirkable responsibility. The report holds that as China and the United States are working toward the establishment of a new type of major-power relationship, cooperation in cyberspace should be an important part of that endeavor.
I. Introduction

Whatever methods of production humankind adopts, the corresponding form of warfare will appear. With the development of information technology (IT), cyberspace is becoming another battlefield following the land, the sea, the air and the outer space. The Internet has become an integral and important part of a state, a society and the daily life of individuals. Moreover, it has gained momentum for further development. Together with the conveniences the Internet has brought to us, it has also entailed an increasing number of potential risks and challenges. For example, the number of cyber-attacks in 2011 increased by 36% as compared with that in 2010, and the amount of malicious software has increased 41% during the same period. China’s white paper on national defense issued in 2013 points out,

“Changes in the form of war from mechanization to informationization are accelerating. Major powers are vigorously developing new and more sophisticated military technologies so as to ensure that they can maintain strategic superiorities in international competition in such areas as outer space and cyberspace.”

Just as in other domains, to maintain order in cyberspace is becoming the international community’s consensus. An American scholar argues that the command of cyberspace in the 21st century is as decisive as the command of the sea in the 19th century and the command of the air in the 20th century. With only about 50 years of history, the Internet is expanding globally at an extraordinary speed. Cyberspace has become a new platform for political, economic, military, and cultural interactions as well as a significant domain that influences social stability, national security, economic development and cultural communication. In reality, cyber-attack and cyber-defense can be conducted at the state level, such as offensive and defensive actions organized by the military, or at the personal level by an individual. It can be a simple hacking
attack, or a long-term, large-scale and state-launched operation aimed at damaging the infrastructure of an enemy state so as to achieve the strategic purpose of paralyzing the running of that state.

There is no unequivocal definition of cyber-attack yet, but it generally refers to unauthorized intrusion into a computer or a computer network in such forms as tampering, denial of service, data theft, and server infiltration. The emergence and development of the non-state cyber groups that are obviously politically-oriented, such as Anonymous, and other cyber crime groups, also add to the complexity of cyber-attacks. It is believed that all the top 15 countries around the world in terms of military budget are developing cyber offensive and defensive capabilities. In 2011, among the 193 UN member states, 68 countries had cybersecurity projects. However, in 2012, the number of such countries increased to 114, among which 47 countries had military cybersecurity projects. These 47 countries are assessing their military capabilities in cybersecurity while developing corresponding military theories. Against such a background, cyberspace arms control is becoming an important part of international arms control and disarmament. However, the number of current measures for arms control in this area is almost zero, which further highlights the importance of international negotiations on the code of conduct in cyberspace as early as possible so as to work out a treaty to regulate international cyber activities.

The developed countries headed by the United States have formulated relatively complete systems of cyber-warfare policies and strategies by making full use of their advanced information technology and sufficient funding. Besides that, they are accelerating their pace in building cyber forces and conducting theoretical research on cyber-warfare. As one of the major creators of the international order after World War II, the United States plays an irreplaceable leading role in international arms control and disarmament. Every single measure and action it takes in cyberspace will inevitably have a bearing on the development of international arms control in cyberspace in the future. This report focuses on such issues as the discussions on cyber-warfare in the international community and the restraints on cyber-warfare imposed by the existing international law. It has also analyzed in detail the preparations for cyber-warfare and the demands for cybersecurity of the United States and a few other countries, and proposed that a new system and normative
rules for cyberspace arms control be established in order to avoid the abuse of cyberspace and not to trigger international conflicts, for which the United States has unshirkable responsibility.
II. Cyberspace and War

Just like the human nervous system, the Internet has extended and permeated the political, economic, military, cultural and social life of various countries across the world. However, the risks that the Internet poses are inherently associated with its convenience and those risks have brought much inconvenience and even trouble to people’s life. In recent years, various kinds of cyber-attacks have occurred more frequently and the harmfulness of cyber-attacks to society has become increasingly conspicuous. Meanwhile, the tendency that war will extend to cyberspace has also caused lots of discussions and concerns.

A. The extension of war to cyberspace

The concept of cyberspace was initially put forward by American scientists, which refers to the electromagnetic space of networks. Originating from the development of computer and network technology, it is a revolution both in technology and in people’s lifestyle. The Transmission Control Protocol and the Internet Protocol (TCP/IP), which evolved from a packet switching network in late 1960s, has completely changed the traditional forms of communication, and the Internet has rapidly spread to the whole world based mainly on cable transmission. As soon as it emerged, the platform of cyberspace has been developing at an amazing speed toward the integration of networks and electromagnetic space and has greatly expanded the physical space for human activities. After over four decades’ evolution, war is also being gradually extended to cyberspace. The Joint Doctrine for Information Operations published by the U.S. military in 2006 pointed out that due to the continued expansion of wireless networking and the integration of computers and radio frequency communications, there would be operations and capabilities that blur the line between computer network operations (CNO) and electronic warfare (EW).

1 徐龙第[Xu Longdi]: 《数字空间硝烟起——怎么看网络安全新边疆》["Hints of War in Cyberspace: How to Observe the New Frontier of Cybersecurity"], 载于《国际热点怎么看》[How to Observe the International Hot Spots], Beijing: World Affairs Press, 2013, pp.136-152.
The extension of war to cyberspace also results from informatization of the human society. Information technology has been widely used in social life since the 1990s. In February 1993, shortly after his inauguration, U.S. President Bill Clinton said explicitly during his visit to the Silicon Valley that the U.S. government would build a national Information Superhighway. Following the United States, countries like Japan, the United Kingdom, Canada, Singapore, India, South Korea, Brazil and Argentina also started similar projects and invested heavily. As information technology quickly became popular in its civil application, it was also extending to military fields. In the same year when President Clinton proposed to build the Information Superhighway, John Arquilla and David Ronfeldt with the RAND Corporation claimed that “cyberwar is coming!”\(^2\) Other countries also put forward such concepts as information operations in the 1990s and took the view that information operations would bring their potential capabilities into full play and improve the efficiency and effectiveness of military operations by combining information from various sources, and that when the information advantage reaches a certain degree, it would enable the advantaged side to make use of the information system and capabilities to gain operational advantage in conflicts or take control of the situation in non-combat military operations while at the same time preventing the enemy from gaining such capabilities.

In the contemporary information era, the Internet has become an important platform and battle space both for civil and military purposes. As early as in 1988, University of California experienced a computer virus intrusion which caused the breakdown of its computer system. The U.S. military soon noticed that together with its great convenience, the Information Superhighway could also exert enormous harmful impact on security because there were serious loopholes in computers, databases, software, operators, routers, data transmission, etc. Such loopholes resulted from the openness of the Internet and the immaturity and rapid development of information technology. Similar incidents that happened later include the following ones: (1) In 1992, the fiber-optic cable of the U.S. Federal Aviation Administration was cut, which caused the computer systems of four of its air traffic control centers to shut down for 35 hours and more than 1,000 flights to be delayed or cancelled; (2) In January 2009, a computer in the internal computer

network at the French Navy was intruded by a computer virus, which quickly spread to the whole network and caused all Navy fighter planes to be “unable to download their flight plans” and grounded for two days.

At the beginning of the 21st century, the U.S. government and military incorporated cyberspace into their horizon and regarded cyberspace as “a global domain within the information environment, which is composed of the interconnected network of IT infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers.” The Cyberspace Policy Review released by the U.S. government in May 2009 also held that cybersecurity risks posed one of the most serious economic and national security challenges to the United States. Therefore, the United States kept on accelerating preparations for cyber-warfare and dramatically increased spending on the development of cyber offensive weapons.

Since 2010, there has been increasingly heated debate about cyber-warfare in the U.S. political, academic and media circles. Richard Clarke, former U.S. cybersecurity czar, once served as Special Advisor to President George W. Bush on cybersecurity. In his book Cyber War: The Next Threat to National Security and What to Do About It, Richard Clarke pointed out that cyber war had begun and the cyber-attacks some countries had suffered were its proof, and that cyber war had serious consequences and could rapidly go global. Mr. Clarke also said that it was only states that were truly capable of waging a cyber war, though the development of information technology enabled some groups and individuals to have unprecedented capabilities. In his article “Defending a New Domain: The Pentagon’s Cyberstrategy” published in Foreign Affairs in 2010, former U.S. Deputy Secretary of Defense William J. Lynn III revealed that the Pentagon had built layered and robust defenses around military networks and was working with the Department of Homeland Security to protect government networks and critical infrastructure and with the United States’ closest allies to expand these defenses internationally. It seems that war is extending to cyberspace at a quickened pace.

---

B. Controversy over the existence of “cyber-warfare”

Cyber-warfare, as an extreme form of cyber threat and cyber-attack, has attracted increasingly extensive attention. As a matter of fact, since the Internet came into being, there have been constant discussions and controversy about cyber war in the international community and various countries have competed with one another to gain the “command of cyberspace”. Computer network tools played an important role in the Gulf War in 1991, the Kosovo War in 1999 and the Iraq War in 2003. In recent years, many countries have taken a diverse range of measures to enhance their cyber-warfare capabilities, such as adopting policies for cyberspace, working out cyber strategies, establishing cyber commands and strengthening the building of cyber forces. Those countries’ moves have given people a sense of feeling that the cyber war is imminent. However, there are different definitions and understandings of war, and cyber-warfare is also interpreted in different ways. In fact, there are a great variety of cyber activities whose nature can hardly be easily determined. Up to now, no agreement has been reached on the definition of cyber threat and cybersecurity. For example, in a report submitted to the European Parliament’s Committee on Foreign Affairs in February 2009, Paul Cornish at Chatham House, or the Royal Institute of International Affairs, classified cyber threats into four levels: hacking; serious and organized crime; ideological and political extremism; and state-sponsored cyber-aggression. According to Alexander Klimberg and Heli Tirmaa-Klaar, cyber-attacks include hacking, Distributed Denial of Service (DDoS), Trojans, etc. Scott J. Shackelford, however, reckons that cyber-attacks are often broken down into four categories: cyber terrorism, cyber war, cybercrime, and cyber espionage. Although virtually every terrorist group has a web presence, true cyber terrorism remains rare and there has not yet been a genuine cyber war. He believes that the most pressing problems are cybercrime and cyber espionage. Michael Glennon observes that any form of cyber-attack is a kind of cyber-intrusion and the danger of cyber-intrusions ought not to be underestimated since

---


they have caused and will continue to cause widespread harm.\(^8\)

Generally speaking, there is no consensus on the existence of cyber-warfare yet. Some hold that cyber-warfare really exists and has begun; others argue that cyber-warfare does not exist and hasn’t happened.

There have been so many discussions and reports about cyber-warfare that it seems to be already an established fact. Just as mentioned before, as early as in 1993, the RAND Corporation’s John Arquilla and David Ronfeldt declared that “cyberwar is coming!” As William J. Lynn III pointed out, “Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space.”\(^9\) Richard Clarke holds that cyber war has made the 9/11 terrorist attack pale and he urged taking a number of measures “simultaneously and now to avert a cyber war disaster”. In February 2011, then Director of the Central Intelligence Agency (CIA) Leon Panetta warned the U.S. Congress that “the next Pearl Harbor could very well be a cyber-attack”. However, some people regard this as a kind of “cyber-mania”, an overreaction to cyber-attacks.

Unlike such “cyber-mania”, Thomas Rid from King’s College London argues that cyber war has never happened in the past, it does not take place at present, and it is unlikely to occur in the future, despite that many cyber-attacks have happened. The reason, according to Thomas Rid, is because an offensive act must meet some preconditions to constitute an act of war. According to the definition given by Carl von Clausewitz, war is violent, instrumental and political. In other words, any act of war must be potentially deadly, instrumental and political. But not one single cyber offense on record constitutes an act of war on its own, no matter it is minor or serious. On the contrary, all politically motivated cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion.\(^10\) David J. Betz, who is also from King’s College London, and Collin S. Gray, a famous contemporary American strategic thinker, hold similar opinions with Thomas Rid and consider many ideas on “cyber war” as simply metaphorical and lacking accuracy in their definition. They believe that cyber tools are only part of war, and cyber war has not come yet.\(^11\)

---


In practice, the U.S. military now classifies cyber-warfare into three levels. At the first level, radio is employed to disrupt, destroy and even control the military electronic system of adversaries. At the second level, small-scale cyber-attacks are launched to coordinate and support conventional operations of war or to give warnings. At the third level is all-out cyber war. Different from media report and the rhetoric of government officials, such a classification is relatively “practical”, at least in the sense that cyber war is associated with the military.

The above analysis reveals that there are still disagreements over the existence of cyber-warfare at present, and the reason is no consensus has been reached on the concept of cyber-warfare and it’s not easy for people to reach agreement on that in a short period of time. However, it is an undisputed fact that cyber-attacks have the potential to cause damage. The series of cyber-attacks that have happened in recent years also seem to serve as hints of war in cyberspace.
III. Cyberspace and Arms Race

The information and communications technology (ICT) has been developed and applied at an extraordinarily fast speed, but people have obviously lagged behind in understanding its political, economic, social and military impact. For example, with regard to the application of information technology in the military field, the actual practices of various countries have gone in advance of relevant theoretical discussions and intellectual constructs. Although more caution is required when we make the judgment that cyber war is reality, the frequent occurrence of cyber incidents has made countries across the world extremely sensitive to the military dimension of cyberspace. Therefore, many countries have taken a variety of measures in recent years to enhance cybersecurity. As a result, there is a clear tendency toward militarization and weaponization of cyberspace and a cyber arms race.

A. Frequent occurrence of quasi-cyber war

Although there is disagreement over the existence of cyber war and no consensus is likely to be reached on its definition in the near future, the application of information technology and the Internet in military fields is not novel and many countries have used them for a number of times in real wars. In other words, information technology and the Internet have become one of the means and instruments of modern warfare and even part of the whole battlefield, somewhat similar to electronic warfare, information warfare and network-centric warfare that people often talk about. However, the widespread existence and application of the Internet has expanded the connotations and denotations of such concepts as “electronic warfare” and “information warfare”. Therefore, even if there is no act of cyber war in a strict sense, many cyber-attacks that have happened might be regarded as quasi-cyber war.12

12 As there is controversy over the understanding of cyber war, it might be more appropriate to call the numerous cyber-attack incidents that have already happened “quasi-cyber war”.
As early as in the Gulf War in 1991, the United States managed to implant computer viruses through its intelligence system into Iraq’s air defense system. Those viruses were activated by remote control before the U.S. military carried out its air strike so that the Iraqi air defense system was already paralyzed when the U.S. air force flew over Baghdad. This operation calls people’s attention to computer network operations. In the Kosovo War in 1999, Yugoslavia organized hackers and caused the breakdown of NATO’s military command network with various kinds of computer viruses. In retaliation, the U.S. forces implanted a large number of viruses and deceptive information in the military command network of Yugoslavia as well as in its civil networks, which rendered the Yugoslav air defense system invalid and caused a power cut over a large area with the collapse of communications for several hours. In the Iraq War in 2003, the U.S. military employed cyber-attacks again. Within only a few days in late February, thousands of Iraqis received an email inducing them to capitulate, revolt against their superiors and change sides. During the War, the U.S. Special Cyber Forces launched destructive attacks against the military communication system of Iraq by using more than 2,000 sorts of computer viruses, which resulted in the Iraqi military receiving false information or not receiving any at all. Such incidents all happened during the wars in a traditional sense, in which information and network tools are obviously a sort of warfare means. The aforementioned incidents are generally considered early cases of cyber-warfare.

Unlike being simply a means of traditional war, cyber-attack incidents in recent years seem to be much closer to a “quasi-cyber war”, which further provide evidence for the coming of cyber war. For instance, the cyber-attacks Estonia and Georgia suffered in 2007 and 2008 respectively and the computer worm Stuxnet discovered in 2010 are considered the latest cases of cyber-warfare.

In April 2007, the Estonian government moved the Bronze Soldier monument in the capital city of Tallinn, a Soviet-era World War II memorial, to a more secluded location. Large-scale riots erupted among the Russians in Estonia and the Russian government protested vociferously, straining the relations between the two countries. Around 10 p.m. on April 26, 2007, the Estonian government websites were suddenly flooded by e-information from various parts of the world. Prominent government websites along with the websites of banks, universities, and news media were attacked and paralyzed. Estonia suffered three waves of large-
scale cyber-attacks, which did not end until May 18. Estonia was forced to block all international web traffic and turned its “internet” into an “intranet”. Although later on NATO sent experts to assist Estonia in combating the cyber-attacks, there was not much that could be done. After the incident, Estonia’s Defense Minister Jaak Aaviksoo said at an international conference that cyber-attack is “the unnoticed Third World War”. It is generally believed by western media that those cyber-attacks originated from Russia. Some western cyber-warfare experts even called it the first cyber war in its true sense.

According to media reports, in the conflict between Russia and Georgia in August 2008, Russia took control of Georgia’s network system before launching the war. After the outbreak of the conflict, nearly all the servers in Georgia were frozen, which resulted in the paralysis of internet services of Georgia’s transportation, communications, finance, etc. The Georgian military even could not receive orders from their superiors and the superiors could not get to know the situation on the battleground, which cleared the way for Russia’s military operations.

Of course, due to the great difficulty in tracking the source of cyber-attacks, there is no hard evidence proving that Russia launched the aforementioned two cyber-attacks.

The above two cases of cyber-attacks have the following characteristics:

Firstly, the methods of attacks are more covert. The data of the attacks against Estonia came from computers located in over 70 countries, including the United States. Those computers might have already been infected with “botnets” much earlier. Due to diversity of the source of attacks, it was very difficult for the country under attack to determine who was responsible for launching those attacks, which also give the attackers more room for political maneuver.

Secondly, the attacks were launched at an extremely fast speed. On the first day of the incident, Estonia suffered about 1,000 attacks and the next day the attacks increased dramatically to 2,000 times per hour. On May 9, 2007, the frequency of attacks reached its peak with Estonia suffering attacks from 4 million data packets per second. The enormous amount of data and high-frequency attacks caused a heavy burden for the servers, which were paralyzed one after another. Before the government and relevant authorities realized what had happened, their cyber defense had been broken through and the attackers reached their objectives of cyber raids.
Thirdly, a wide range of targets were attacked. In the two cases of cyber-attacks, almost all the Internet platforms of important branches in the two countries were attacked, such as the government, the military, media, banks and schools. While cyber-attacks caused great difficulty in command of the military, they also brought great chaos to the normal functioning of societies.

Up to now, the computer worm Stuxnet can be said to have made the most serious physical or real impact. In November 2010, the Stuxnet worm attacked the nuclear facilities in Iran, such as the uranium enrichment plant at Natanz, and caused radiation leak at the Bushehr nuclear power plant constructed by Russia. The experts’ analysis of Stuxnet revealed that it was a specially designed computer virus that targeted centrifuges, but after “appropriate adjustments” it could attack industrial control systems all over the world. This virus has complex code and is extremely difficult to identify. It can force a change in the centrifuge’s rotor speed, inducing excessive vibrations or distortions that would destroy the centrifuge. Although the Stuxnet worm did not destroy Iran’s nuclear facilities, it severely damaged about 20% of Iran’s centrifuges, thereby greatly delaying the implementation of Iranian nuclear program. It is generally believed that the creation of Stuxnet worm was a joint effort by the United States and Israel. The birth of the Stuxnet worm symbolizes the emergence of another cyber weapon and cyber war has entered a new phase. According to an investigative article in *Vanity Fair*, “Stuxnet is the Hiroshima of cyber-war.”

According to the aforementioned Clausewitz’s three-attribute definition of war, this cyber-attack may be the closest act to that of “cyber war”. To begin with, there was a conspicuous political motivation behind the incident. In a situation where Iranian nuclear talks reached a stalemate, Tehran was not supposed to renounce its right to nuclear development and the cost of an overt military intervention appeared to be prohibitively high and its outcome unpredictable, cyber-attack became a relatively safe action, which would delay the implementation of Iran’s nuclear program or damage its nuclear facilities, and all that at relatively low political costs without incurring all sorts of unpredictable consequences a military strike might cause. Another reason is that the cost of research and development for such complex viruses as Stuxnet is so high that it would not have been possible if not sponsored by a State. The financing capability of hackers is by no means comparable to a State.

---

Secondly, the specially designed and adapted Stuxnet worm is both aggressive and instrumental. Before the recent revelation, the virus had been running for up to seven years from November 2005 to June 2012. By the end of 2010, the virus had infected nearly 100,000 hosts in a number of countries, 60% of which are located in Iran. However, the virus did not destroy all infected hosts, because its choice of prey was very strict - only two models of Siemens logic controllers, namely, 6ES7-315-2 and 6ES7-417 were targeted. If no configurations indicative of these two types were detected, the Stuxnet would not activate and no harm would be inflicted on the host computers.  

The third aspect is where doubt and disagreement occur. It concerns whether or not the Stuxnet worm possesses a violent attribute. Computer virus, per se, does not have a violent attribute, or the destructiveness comparable to conventional explosives. Also, as some had put it, although the Stuxnet worm destroyed 20% of Iran’s centrifuges, yet there were still 80% unaffected. This is believed to be proof that its impact was limited and that Iranian scientific expertise and research capability had not been undermined as a result. A more important fact and a more relevant theme reoccurring in discussions on cyber-warfare is that the Stuxnet worm did not cause casualties, let alone heavy ones. In fact, neither the Stuxnet nor any other cyber-attacks have resulted in grave consequences involving human casualties. In this sense, it would be inappropriate to say that cyber-attacks possess a violent attribute, hence the predicament the victims may find themselves in when they are to decide if they should take countermeasures (including military measures) to respond to cyber-attacks and how. Therefore, according to the narrow definition by Thomas Rid, even this cyber incident cannot be termed as an act of “war”; but anyhow it was still a “quasi-cyber war”, the closest one to the strict definition of cyber war.

Coincidentally, the Russian cybersecurity software maker Kaspersky Lab released a report on May 28, 2012, claiming that they found the Flame virus, a more complex and advanced one than the Stuxnet. It was found to be spreading widely across the Middle East, where Israel, Syria and some other Middle Eastern countries were affected with Iran hit the hardest. The virus was able to store specific information, such as the host computer’s information related to nuclear industry,

---


15 徐龙第 [Xu Longdi], 《战争法在网络空间的适用性：探索与争鸣》 [*Applying the Law of War to Cyberspace: Exploration and Diversity of Views*], 载于 《当代世界》 [*Contemporary World*], Issue 2, 2014.
and then proceed with perpetrations of monitoring, interception and even sabotage. Technicians with the Lab categorized the Flame virus as a “heavy cyber weapon”, and speculated that a nation-state is likely to blame for unleashing it on the Internet.

Although the Stuxnet worm and the Flame virus did not cause brutal combats visible to people as in ordinary wars, yet attention should be given to their political and military implications and their international influence.

**B. The increasingly intensifying arms race in cyberspace**

Frequent occurring of cybersecurity incidents has increased the urgency to safeguard cyberspace. To enhance cybersecurity, countries over the world have taken a variety of measures in recent years. Some of them are even building large-scale cyber forces, which in turn intensifies cyberspace arms race and makes it more difficult to maintain order and stability in cyberspace. In addition to the United States, Russia has also started its research on cyber-warfare for long. Early in the 1990s, Russia set up a special Information Security Committee and placed information cybersecurity on an equally important position with economic security. In 1995, Russia incorporated information security into its Constitution as part of national security and enacted the Federal Law on Information, Informatization, and the Protection of Information. In September 2000, Russian President Vladimir Putin formally approved the Information Security Doctrine of the Russian Federation, laying down clearly Russia’s national policy on information security. In 2002, the Russian Information Security Commission passed the Doctrine of Russian Information Security, defining cyber-warfare as the sixth generation warfare. And it put forward approaches and appropriate measures to advance national interests in the field of internet security and prescribed directions for Russian military to prepare for cyber-warfare. The Russian armed forces attaches great importance to cyber war preparedness in thoughts. Because of its emphasis on “defeating enemies

---

16 Relevant information on the United States is provided in the following chapter.  
17 The sixth generation warfare is proposed with reference to the previous five generations of warfare. Earlier generations of warfare evolved from fighting with infantry and cavalry forces (first generation), then with black gunpowder and muskets (second generation) and later with rifled arms and tube artillery (third generation). The fourth generation was introduced with heavy weapons, including among others missiles, aircrafts, warships, tanks and armored vehicles. The fifth generation warfare refers to nuclear warfare. See 严涵 [Yan Han], 《第六代战争》[“The Sixth-Generation Warfare”], 载于《航空世界》[Aviation World Monthly], Issue 2, 2003; 《各国摩拳擦掌密部署网络战：未来第六代战争》[“Various Countries Make Thorough Preparations for Cyber War: The Future Six-Generation Warfare”], 载于《南方日报》[Nanfang Daily], January 9, 2012.
by the first opportunity”, they advocate taking the initiative in attacking adversaries and stress the necessity of obtaining information and electromagnetic dominance over its adversaries. To ensure an advantaged position in cyber conflicts, the Russian military has set up information forces specialized in protecting networks and launching cyber-attacks. Russia also leads the way in developing network technologies and cyber weapons. It is reported that Russia not only possesses advanced cyber weapons such as wireless data communication jammers, logic bombs and worms, network data-collecting computers and reconnaissance tools, and embedded Trojan time bombs, but also has put them into operation. For instance, both Estonia and Georgia condemned Russia for launching cyber-attacks against them. Recently, the Russian military has set new goals: Firstly, setting up a cyber force capable of both attack and defense; Secondly, building up “cyber deterrence” so as to ensure their cyber-warfare capabilities play the role of a powerful deterrent before the outbreak of cyber conflicts; Thirdly, highlighting the role of media and information war, including media battle and electronic interference for the purpose of being best prepared for cyber-warfare in both theory and practice. Meanwhile, Russian hackers enjoy a “reputation” in the world. With regard to private networks and instant networking, Russian experts are developing various computer viruses, especially the “long-distance wireless injecting virus weapons”, which can pose direct threats to the command and control system of hostile forces. The U.S. Defense Information System Network estimated that Russia has a cyber force of more than 7,300 people, with a military budget of US$40 billion.

In response to the rapid emergence of cyber-warfare, other countries in the world are also taking active actions. Britain, South Korea, Japan, India and Israel are all intensifying their studies in cyber-warfare and have set up cyber-warfare units or forces. Hence arms race in cyberspace has become increasingly intensified. In 2001, Britain secretly set up a “hacker force” composed of hundreds of computer elites, under the command of Military Intelligence, Section 6 (MI6). It also works closely with the United States and Canada to set up cyber forces with the purpose of advancing research in computer viruses, “hacker” attack and other related aspects. In June 2009, Britain released the UK Cybersecurity Strategy, planning to recruit cybersecurity professionals, including hackers, to safeguard its cyberspace. It also

---

announced the establishment of the Office of Cyber Security (OCS) and the Cyber Security Operations Center (CSOC), respectively responsible for coordinating the UK’s cybersecurity policy, and monitoring the Internet for threats to British infrastructure and launching counter-attacks when necessary.

In 1999, South Korea laid down a general plan for future information development, and in 2009, it announced that a “cyber command” would be established, which was put into operation in 2010. Presently, South Korea possesses about 200,000 trained professionals and invests annually 5% of its defense budget in the development of cyber-warfare technology. It is reported that the South Korean Defense Ministry has already set up a special force for cyber-warfare – Anti-hacking Force, recruiting tens of thousands of information warfare professionals. South Korea also plans to expand on a large scale the force of its Cyber Command, amounting to 1,500 people.19

Japan tries to paralyze its adversaries’ combat system by achieving “cyber dominance”. In constructing its cyber-warfare system, Japan attaches great importance to developing both offensive and defensive capabilities. To enhance such capabilities, Japan has invested huge amount of funds into its network hardware and “cyber forces”, setting up the Defense Information Communications Platform and the General Platform of Computer Systems in order to achieve information exchange and resources sharing among network systems in different agencies and military units of the Self-Defense Force (SDF). Japan’s Defense Ministry has established a cyber defense force of 5,000 people, dedicated to attacking and defending network systems. Currently, Japan’s cyber defense force is quite powerful in its cyber war operations. The country also stresses its cooperation with the United States by introducing advanced technologies into its own development with a view to perfecting its technology and to enhancing its cyber-warfare capabilities.20

In recent years, India has fuelled more financial support to the hardware development of cyber-warfare and given full play to its advantages in software research. It has developed and introduced state-of-the-art servers, firewalls and supercomputers and has made active preparations for cyber war. Presently, the

---

Indian military has set up a joint computer emergency response unit composed of the army, the navy and the air force, recruiting top-level “hackers” to gradually fill the talent pool for future cyber-warfare. Adhering to the principles of self-reliant research and development and civil-military cooperation, India strives to build up its own system in the fields of network technology, encryption technology, chip technology and operating systems by investing huge amount of manpower and material resources. The establishment and application of Flash Messenger high-speed broadband network and the Third Eye navy confidential data transmission network will further consolidate the asymmetric advantage of the Indian military in fighting future cyber war. In addition to improving its defense systems, the Indian military has also put cyber-attacks into its fighting doctrine and proposed unequivocally to establish a network system that can disable not only the command and control system but also the weapon system of its adversaries, and to set up cybersecurity agencies in Army Headquarters, all area commands and important military departments.\(^\text{21}\)

**C. Preparations of the United States for cyber-warfare**

James Adam, a U.S. military forecaster, once predicted that “the computer would be a weapon in future wartime and there would be no virtual front line as traditional battles have, and that bits and bytes would replace bombs and bullets as the crucial instrument to seize control of the battlefield”. The RAND Corporation also pointed out in one of its reports that “the strategic war in industrial age is nuclear war, while in information age the strategic war is mainly cyber war”. In fact, the United States has prepared for cyber conflicts for a long time. To confront possible cyber-attacks or cyber-warfare, it has, in recent years, sped up its efforts and pace in forming cyber forces and given full play to its advantages in technology, policy and management mechanisms.

1. **Formulating policies for cyber-warfare**

   The United States has issued a series of policy documents in the 21st century,

\(^{21}\) 安亮[An Liang], 《虚拟世界，战争动员已打响——从英政府关闭社交网站举措看外军信息网络动员》[“The War Mobilization Has Started in the Virtual World: Observing Information Network Mobilization of Foreign Military from British Government’s Closing of Social Networking Sites”], 载于《解放军报》[PLA Daily], August 18, 2011.
laying down the guidelines for its preparation for cyber-warfare. In 2002, U.S. President George W. Bush signed a secret order – National Security Presidential Decree No.16, instructing the U.S. Department of Defense (DoD) to take the lead in formulating a strategy for cyber-warfare in order to enhance its offensive and defensive capabilities in cyberspace. In 2003, U.S. Defense Secretary Donald Rumsfeld approved a secret DoD report entitled “Information Operations Roadmap”, requiring U.S. military to seek complete dominance in the information spectrum by possessing the capability to destroy telecommunication systems, radars and all electromagnetic-based weapon systems across the world. In 2005, the United States set up its Joint Functional Component Command – Network Warfare (JFCC-NW) to coordinate its offensive computer network operations, and the Army, the Navy, the Air Force and the Strategic Command all established their cyber commands. In March 2005, the Pentagon issued the National Defense Strategy, explicitly defining cyberspace as important as the land, the sea, the air and the outer space, the fifth space over which the United States need to maintain a decisive control. In 2007, when formulating the National Military Strategy for Cyberspace Operations, the U.S. Air Force defined cyberspace for the first time as a domain accessible for military operations. In May 2009, the United States completed its Cyberspace Policy Review, the contents of which were reiterated by the U.S. National Security Strategy released in 2010. In October 2012, U.S. President Barack Obama signed a presidential decree concerning cyberspace military operations, and as a classified document, its contents remain a mystery.

On February 12, 2013, Barack Obama signed an executive order entitled “Improving Critical Infrastructure Cybersecurity”, which called for more rigorous protection of critical infrastructure against cyber-attacks. It also tasked the federal agencies to establish a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing, including the dissemination of classified reports to critical infrastructure entities authorized to receive them. The new executive order requires the Secretary of Commerce to direct the Director of the National Institute of Standards and Technology to lead the development of a framework to reduce cyber risks to critical infrastructure within one year. The so-called “critical infrastructure” refers to systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security,
national economic security, national public health or safety, or any combination of those matters. As most U.S. critical infrastructure facilities are run by private entities, the fundamental significance of this executive order is government’s involvement in business operation. Using public power in the private sector is to tighten up government’s control over networks. However, whether American private companies are willing to work hand in hand with their government is not only a security issue, but concerned with U.S. conventional business operation model. Whatever the outcome may be, the forceful interference into private business operation has become an important step of the U.S. government to safeguard cybersecurity. The aforementioned policies have prepared the United States with strategic guidance and theoretical foundation for fighting cyber war, enabling it to carry out practical operations in accordance with laws and regulations. That is what food and fodder (ideas) should go ahead of troops and horses (actions).

2. Setting up institutions and mechanisms

The United States has set up its Cyber Command specifically responsible for cyber-warfare, which went ahead of other countries in terms of cyber operation mechanism. In June 23, 2009, U.S. Defense Secretary Robert Gates officially announced the establishment of U.S. Cyber Command (USCYBERCOM) with a staff of a thousand people, subordinate to U.S. Strategic Command. The U.S. Cyber Command integrates command authorities of cyber operations in all services and enhances the cooperative engagement capability of various agencies so as to accomplish the new mission of obtaining dominance in cyber-warfare. In October 2010, the U.S. Cyber Command came into full operation and was composed by several service components, i.e. Army Forces Cyber Command, 24th U.S. Air Force, Fleet Cyber Command and Marines Forces Cyber Command. The establishment of U.S. Cyber Command not only achieved single command of U.S. forces cyberspace operations, but also strengthened their cyber-warfare capabilities. Hence cyber war becomes an independent operation mode. The Washington Post reported in January 2013 that the Pentagon approved a major expansion of its cybersecurity force over the next several years, increasing the size of U.S. Cyber Command more than fivefold, from the present about 900 personnel to 4,900 troops and civilians, so as to bolster remarkably U.S. ability to defend critical computer systems.22

On December 18, 2012, U.S. Secretary of Defense Leon Panetta said that the DoD had developed new rules of engagement in cyberspace, i.e. operations doctrine for cyber forces, that clarify U.S. armed forces’ mission to defend the nation and would enable them to more quickly respond to cyber threats. He added that the DoD was looking at ways to strengthen the Cyber Command, ensuring that it has the resources, the authorities and the capabilities required to perform its growing mission. In accordance with the order of President Obama, U.S. Cyber Command, originally taking the responsibility to deal with threats to the infrastructure of military networks, is responsible for wider domains - the defense of national networks. In November 2012, the U.S. Defense Advanced Research Projects Agency (DARPA) released a document entitled “Basic Network Warfare (Plan X)”. The document claims that the Plan X “will conduct novel research on the cyber domain”, and “attempt to create revolutionary technologies for understanding, planning and managing DoD cyber missions in real-time, large-scale and dynamic network environments”. To achieve that goal, the Plan X system “will be developed as open platform architecture for integration with government and industry technologies”. Currently, the United States has basically completed its comprehensive preparations for full-scale cyber war, both in theory and in real-time combat.

In addition to the Cyber Command, the United States has established other cybersecurity mechanisms, forming a relatively comprehensive systematic framework. At present, cybersecurity affairs of the United States are mainly handled by the Department of Homeland Security (DHS), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI) and the Department of Defense (DoD). The Department of State and the Department of Commerce are responsible for the consultation and standard formulation concerning cybersecurity. The DHS National Cybersecurity Division (NCSD) is responsible for coordination among public agencies, the private sector and international organizations to protect U.S. cybersecurity and cyber interests. The National Cyber Response Coordination Group (NCRCG) composed of 13 federal agencies is responsible for responding to cyber incidents of national significance. The DHS has expanded the working domain of the Office of Cybersecurity and Communications (CS&C) to enhance its awareness of cyberspace situation and information-sharing capability. In October 2010, the DHS and DoD signed a memorandum of agreement regarding
cybersecurity to increase interdepartmental collaboration in strategic planning, mutual support for cybersecurity capabilities development, and synchronization of cybersecurity mission activities. In 2012, the Obama administration proposed to the U.S. Congress twice a draft resolution on authorizing the DHS with the power to protect critical infrastructure networks, but failed to get their approval. In addition, to improve the coordination of cybersecurity operations and policies, the White House appointed its Cybersecurity Coordinator in December 2009, and the State Department appointed its Coordinator for Cyber Issues in February 2011.

3. Developing cyber-warfare capabilities

The United States attaches great importance to the development of its capabilities for cyber-warfare. In 1995, the 16 “cyber warriors of the first generation” graduated from Information Resources Management College, National Defense University. Since then, the U.S. cyber force has grown increasingly strong. The former U.S. Secretary of Defense Robert Gates once proposed that the Pentagon should train four times more cybersecurity experts annually, increasing the number of newly added cybersecurity experts every year to 250. At present, the U.S. armed forces have 3,000 to 5,000 cyber-warfare professionals, with 50,000 to 70,000 soldiers engaged in cyber-warfare. Should the former electronic warfare staff be included, the U.S. cyber force would amount to more than 88,700 people.

The United States has conducted several cyber-warfare exercises. For instance, in 2006 and 2008, it organized and staged “Cyber Storm I” and “Cyber Storm II” exercises which engaged and coordinated 18 federal agencies, and over 40 technology companies, like Cisco and Microsoft, took part. Since Barack Obama was sworn in as U.S. President, he has placed the threat of cyber intrusion against the United States in equivalence to the threats of nuclear and biological weapons. In 2010, the United State, together with 15 other countries, conducted “Cyber Storm III” exercise on an unprecedented scale.

The United States has actively engaged itself in developing and researching cyber offensive weapons. It is reported that the United States is working on or has succeeded in developing hard-kill cyber weapons, such as electromagnetic pulse bombs, infrasonic weapons, anti-satellite laser weapons, kinetic energy interceptors and high-power microwave weapons, to carry out attacks on the physical carriers
of the adversary’s networks. In terms of soft-kill cyber weapons, the U.S. military has developed more than 2,000 computer viruses, by which the U.S. forces can, on the one hand, gather intelligence, and on the other hand, send an avalanche of spam in a short time to its target servers to disable the enemy’s computer systems by causing overload and congestion.

In August 2010, the *Washington Post* reported that the Pentagon was developing a range of weapons capabilities, including tools that would allow “attack and exploitation of adversary information systems” and that can “deceive, deny, disrupt, degrade and destroy” information systems, according to DoD budget documents. On March 19, 2012, the *Washington Post* reported once again that the Pentagon was accelerating efforts to develop a new generation of cyber weapons capable of disrupting enemy military networks even when those networks were not connected to the Internet. Such cyber weapons can target “offline” military systems in part by harnessing emerging technology that uses radio signals to insert computer coding into networks remotely.

The United States has not just vigorously developed its cyber weapons, but has also actively sought and created legal grounds for its use of cyber weapons. In February 2013, according to a report in the *New York Times*, “A secret legal review on the use of America’s growing arsenal of cyber weapons has concluded that President Obama has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad.”

### 4. Providing financial support

The United States does not grudge financing cyber-warfare preparations. In 2011, the Pentagon decided to allocate US$500 million in the next five years to the DARPA to speed up its development of cyber weapons and defensive network technologies. The DoD’s 2012 budget for cybersecurity and cyber technology reached US$3.4 billion. The American defense contractors Lockheed Martin and Boeing have also established cybersecurity divisions, and they estimated that the U.S. Government would have spent US$10.7 billion in its procurement of cybersecurity goods and services by the year 2013. In 2008, the Pentagon spent

---


US$30 billion in building the National Cyber Range, a project as grandiose as the Manhattan Project, for the purpose of safeguarding U.S. cybersecurity, protecting the United States from hostile cyberstrikes and mounting counter-attacks against its adversaries on the Internet. To regulate the application of cyber weapons, the Pentagon has prescribed a list of cyber weapons and tools, dividing them into three categories ranging from global, regional to hostile areas, which provides a basis for the United States to launch cyberstrikes.

The United States has not wasted its efforts in its preparation for cyber-attacks, but is being well rewarded. For instance, identifying the origin of cyber-attacks has always been the biggest technical challenge in confronting cyber threats, and the U.S. officials are quite reticent about their cyber-warfare capabilities. However, in October 2012, U.S. Defense Secretary Leon Panetta told Reuters that the United States was making significant investments in cyber forensics to address the problem of identifying where the attacks came from, and the country was seeing returns on those investments. In the same month, Panetta, while delivering his cybersecurity policy speech for the first time, disclosed that the U.S. forces had the capacity to identify the origin of cyber-attacks and possessed the cutting-edge technology of cyber-attacks, and that if aware of impending cyber-attacks, the United States had the capability to take a “pre-emptive” action. He said,

“Potential aggressors should be aware that the United States has the capacity to locate potential aggressors and to hold them accountable for their actions that may try to harm America. For these kinds of scenarios, the Department [of Defense] has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace.”

A senior U.S. defense official said the United States had attributed thousands of minor cyber-attacks to criminal gangs, foreign nations and individuals, and that although conventional wisdom about cyberspace was that it was impossible to attribute attacks to any specific individual or nation-state, the United States had invested a lot in the Defense Department in developing that capability, and it had improved tremendously.

---


Since June 2013, former U.S. National Security Agency contractor Edward Snowden has disclosed the U.S. mass surveillance program on Internet and telephone metadata - PRISM. If people were still doubtful about the remarks of Panetta or other U.S. defense officials on America’s capabilities to identify the origin of cyber-attacks, the PRISM program has not only demonstrated U.S. cyber capabilities in front of the world, but in a certain sense lent credence to the remarks of Panetta and the like. Just like the PRISM program exposed by Snowden, the U.S. capability in tracing cyber-attacks may be well beyond people’s imagination. However, America’s pursuit of cybertechnology, cybersecurity and hegemony in cyberspace is harmful to the establishment of order in cyberspace and even more destructive to building mutual trust among different countries. In addition, it has intensified arms race in cyberspace, hence posing a great challenge to cybersecurity and strategic stability of the world.

It is obvious that by making full use of its advantages in information technology, the United States has not only abused its legal and technological means in anti-terrorism operations, but put the leaders of other countries, including its allies, and important international conferences under surveillance, all with the excuse of protecting national security. These heads of states are neither terrorists nor the men in the street. The close surveillance of these leaders is to gather political, economic and military intelligence of their countries in a timely manner and to understand in advance the directions these countries are going to take. In this sense, protecting national security is not just counter-terrorism in the eyes of the United States, rather it is to exploit its superiority in information technology to strengthen intelligence gathering so as to maintain U.S. hegemony in the world. The increasing militarization and weaponization of cyberspace has already departed from the general objectives of internet development, and by conducting mass surveillance of the Internet, the United States has gone further on the road of abusing information technology.
IV. The United States and Cyberspace Arms Control

Considering current complex and ever-changing activities on the Internet and extensive cyber threats, it is imperative to formulate rules and regulations to address these threats and safeguard cybersecurity. However, there is no universal international treaty at present to regulate cyber activities and to control the development of cyber arms since cyber-attacks are still in the gray zone in terms of law and strategy. The recent policy debate on the issue has not yielded any international treaty, and what is particularly eye-catching is the attitude and role of the United States during the debate.

A. The attitude of the United States toward cyberspace arms control

As mentioned earlier, the existence of cyber-warfare is still a controversial issue. Although western countries headed by the United States have been very active in exploring cyber-warfare rules, the U.S. attitude toward cyberspace arms control has experienced a transformation from objection to flexibility. There are many reasons for this transformation, including enhancement of U.S. cyber attribution capability, confirmation of its leading position in cyber weapons development (for instance, the success of Stuxnet worm in attacking Iran’s nuclear facilities), deepened understanding of related domestic and international legal issues, bilateral agreements reached on cybersecurity (say, the U.S.-Russia pact to create communication link on cybersecurity), considerations on its foreign strategy and the new progress made by the international community on cyber issues (for example, the consensus document released by the UN Government Expert Team in June 2013).
1. Two ways to regulate cyber conflicts and cyber-warfare

There are two ways to regulate cyber-warfare. The first one is to formulate new rules of international law and sign a new international treaty, such as the International Code of Conduct for Information Security (hereinafter called the Code of Conduct) proposed by China, Russia and other countries. The second way is to make adjustments to existing norms of international law to adapt to cyberspace and cyber-warfare. This way has gained support of the United States, NATO and other countries and organizations.

On September 12, 2011, China, Russia, Tajikistan and Uzbekistan requested the UN Secretary General Ban Ki-moon through letter to distribute the Code of Conduct as an official document in the 66th session of the General Assembly with the aim of discussing the document within the UN framework and reaching consensus on international norms on information and cyberspace as early as possible. Although the document is the first of its kind to put forward comprehensive and systematic proposals on international information and cybersecurity rules, the United States and its allies have largely put it aside and neglected it. Recently, Amitai Etzioni, a senior advisor of the Carter administration, said that if one did not know which nations submitted this proposal, one could easily assume that 95 percent of the draft code was composed by western nations led by the United States. This has clearly shown the universal significance of the proposal.

On the contrary, the United States, NATO and other western countries and organizations take the view that the existing international law can be applied to cyberspace and there is no need to create new ones. This view was formally expressed by U.S. State Department legal advisor Harold Hongju Koh in the Inter-Agency Legal Conference of U.S. Cyber Command held in September 2012. In the same month, NATO issued Tallinn Manual on International Law Applicable to Cyber Warfare (published by Cambridge University Press in 2013, hereinafter called the Tallinn Manual) after three years’ study. This manual illustrated 95 rules that were applicable to cyber-warfare, covering rights and responsibilities of States in cyberspace, the use of force, etc. Moreover, the Tallinn Manual also

27 徐龙第[Xu Longdi], 《战争法在网络空间的适用性：探索与争鸣》["Applying the Law of War to Cyberspace: Exploration and Diversity of Views"], 载于《当代世界》[Contemporary World], Issue 2, 2014.
includes comments on each rule, which reflects the discussions, agreements and disagreements during the drafting process.

No matter which way is chosen, making new rules for cyber-warfare or applying the existing norms to it, we should stick to the original purposes of the law of war, of which the first one is to protect non-combatants (e.g. civilians, medical staff or religious people in the army), and those who have stopped fighting (e.g. the injured, the shipwrecked, ailing combatants, or captives); and the second purpose is to limit the means of war (especially weapons) and the methods of war (e.g. military tactics) so that the impact of armed conflicts could be mitigated. These purposes are also the purposes of cyberspace arms control and cybersecurity rule-making.

2. The U.S. attitude toward cyberspace arms control

To prevent cyberspace arms race and cyber-warfare from happening, Russia, as the first country to do so, raised a proposal on cyberspace arms control. It hoped to reach an agreement with NATO and other military organizations headed by the United States through negotiation. In 1996, Russia and the United States held secret talks on cyber-warfare in Moscow for the first time. As then U.S. head of delegation John Arguilla recalled, he had received almost no interest from within the American military after those initial meetings and “it was a great opportunity lost”.  

In 1998, Russia submitted to the first committee of UN General Assembly (Disarmament and International Security Committee) a draft resolution entitled “Developments in the Field of Information and Telecommunications in the Context of International Security”, which was adopted without a vote. The resolution expressed concern that information technologies and means could potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the security of States. It considered that it was necessary to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes, and called upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security. Since then, the issue of

---

information security has been on the UN agenda, and Russia has been submitting similar proposals to the General Assembly every year. Moreover, there have been annual reports by the UN Secretary-General to the General Assembly with the views of Member States on the issue.\textsuperscript{32} However, these efforts were opposed by the United States repeatedly.

Some cybersecurity incidents that occurred in recent years have made cyberspace arms control one of the hot topics. Although there are still disagreements on the question whether these incidents belong to cyber-warfare in its true sense, they have fully demonstrated that cyber-attacks can cause serious damages to major infrastructure and can be utilized for military purposes, thereby highlighting the importance and urgency of cyberspace arms control. This explains why Russia brought up the issue again when more than 10 years had passed since its proposal was first raised in the UN. In March 2009, Deputy Secretary of Russia National Security Council Vladimir Sokoloff reiterated Russia’s position on cyberspace arms control, including banning insertion of malicious codes and chips by States in a secret way that could be activated in future critical moments in computer systems, forbidding military cyber-attacks toward non-combat personnel and units, strengthening supervision of the Internet by Governments, etc.

In September 2011, Russia, China, Tajikistan and Uzbekistan proposed the Code of Conduct which had not aroused the interest of the United States. A U.S. State Department official said, “They [Russians] want to constrain offense”, but “we needed to be able to criminalize these horrible 50,000 attacks we were getting a day”. Some Americans hold contrary opinions to that of Russians. For instance, Stewart Baker, a former employee of the Department of Homeland Security, said that it was impractical to formulate global rules on cybersecurity and internet privacy protection because violation of these rules could bring lots of benefits.\textsuperscript{33}

In 2009, President Barack Obama appointed the White House’s Cybersecurity Coordinator, responsible for coordinating information security activities across federal government agencies. Some people regard the appointment as a major shift of U.S. policy on cybersecurity, which shows that the Obama administration is going to treat its promise on cybersecurity seriously. In July 2010, 15 countries, including the United States, the United Kingdom, China and Russia, agreed to

\textsuperscript{32} “Developments in the field of information and telecommunication in the context of international security”, United Nations Office for Disarmament Affairs (UNODA), http://www.un.org/disarmament/topics/informationsecurity/.

\textsuperscript{33} He also opposes European Data Protection Directive, regarding it as a new kind of colonialism that attempts to impose the concept of privacy to the world.
cooperate for reduction of cyber-attacks, and the United States agreed to join the cooperation for cyberspace arms control in the UN framework so as to address the issue of cyber-warfare. The 15 countries suggested formulating an acceptable code of conduct for cyberspace by the United Nations, exchanging information on national legislation and cybersecurity strategy and building the capacity of least developed countries in protecting their computer systems.

All these trends manifest that the United States is rethinking its objection to cyberspace arms control. Robert Knake, a cyber-warfare expert at the Council on Foreign Relations (CFR) believes that the U.S. participation in the UN Group of Governmental Experts on Cyber Issues marks a major shift of the U.S. attitude toward cyberspace arms control, which proves that the Obama administration has implemented its “engagement” strategy. The U.S. Cyber Commander and Director of the National Security Agency (NSA) Keith Alexander said that “Russia’s proposal can serve as the starting point of international debate” and that “this is an issue that we should and are about to think over”. So some people think it is not impossible for the international community to reach consensus on Russia’s proposal for preventing cyber war.

In June 2013, the United States and Russia signed the Cooperation Agreement on Information and Communications Technology Security after over two years’ negotiation. Both parties agreed to set up a new working group, under the auspices of the Bilateral Presidential Commission, dedicated to assessing emerging ICT threats and proposing concrete joint measures to address them. The two countries have also agreed to take ICT Confidence-Building Measures (CBMs) to increase transparency and strengthen links between the U.S. Computer Emergency Response Team (CERT) and its Russian counterpart for sharing cyber threat indicators. These exchanges can help expand the volume of technical cybersecurity information available to the two countries and improve their ability to protect the critical networks. Moreover, the two sides decided to use the Nuclear Risk Reduction Center (NRRC) links established in 1987 between the United States and the former Soviet Union to exchange information so as to reduce the possibility of misconception and escalation from ICT security incidents. Furthermore, the White House and the Kremlin authorized a direct secure voice communications line between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council in case of a need to directly manage a crisis situation arising
from an ICT security incident. Before signing the agreement, the U.S. and Russia had exchanged white papers, unclassified ICT strategies and other relevant studies. All these measures are conducive to increasing transparency and building mutual trust between the two countries.34

However, considering the overall situation of cybersecurity and the uncertain prospect of reaching an international agreement on the issue, many people reckon that these confidence-building measures are just transitional or intermediate actions before signing a formal treaty on cybersecurity (or cyberspace arms control). In any way, the United States and Russia have taken a significant step for enhancing mutual trust in cyberspace. Unfortunately, the PRISM program was exposed in June 2013 by Edward Snowden, a former U.S. National Security Agency (NSA) contractor, who later escaped to Russia and obtained one-year asylum there. This incident has caused great difficulties to U.S.-Russia relations and cast a shadow on the improving bilateral cyber relations as well as the process of international cyberspace arms control. It is likely that the struggle between the United States and Russia on Snowden’s asylum or repatriation will continue.

Apart from various practical considerations of the United States, there are also some objective factors that hinder the progress of cyberspace arms control. The first is strategic conflicts. Different countries have different strategic purposes for cyberspace and that makes cyberspace arms control an arduous task. The power game between the United States and Russia is an example in that sense. The second is the difficulty in defining related concepts. Currently, there are tremendous disagreements within the international community over the definition of such concepts as cyber weapons, cyber-attacks and cyber-warfare, which makes it very difficult to discuss the issue of limiting the development of cyber weapons and cyber armament. The third is technological problems, especially the difficulty in attributing cyber-attacks to a particular country, organization or individual. For that reason, added by the virtual nature of cyber weapons, it is really difficult to establish an effective verification mechanism for arms control in cyberspace. The last factor is the allure of cyber weapons’ military functions. At present, the potential of ICT has not been fully recognized yet, and the political and military benefits of the ICT seem to be limitless. Under such circumstances, we can hardly

see any sincerity in the negotiations for cyberspace arms control. Unless cyber-attacks bring about humanitarian catastrophes or seriously threaten global strategic stability and security, cyberspace arms control can hardly gain momentum, and when that happened, calling for cyberspace arms control would be too late.

From the above analysis we can conclude that the U.S. attitude toward cyberspace arms control is somewhat ambivalent, and it has undergone some changes and will change further in the future. The objective of cyberspace arms control is to prevent global arms race in cyberspace. However, it requires many painstaking efforts, in-depth discussions and a fairly long period of time to reach broad consensus and to negotiate a binding international treaty on the issue.

**B. The struggle for rule-making power in cyberspace arms control**

It is difficult to advance cyberspace arms control because cyberspace is a new field with relevant international rules not established yet on the one hand, and on the other hand, cyberspace has become a brand-new platform for competition, conflicts and cooperation among various countries, particularly major powers. To safeguard cybersecurity and regulate online activities of various actors, many people and international organizations have been appealing countries to sign global cyberspace agreement or treaty. However, the struggle for rule-making power as the core of cybersecurity/cyberspace arms control game will last for a long time.

**1. Competing cybersecurity policies**

Just as in other policy areas, due to differences in such aspects as historical and cultural backgrounds and the stage of economic development, different countries have different policies and interests in internet development and cybersecurity. For example, British Foreign Secretary William Hague proposed seven principles underpinning future international norms about the use of cyberspace: (1) The need for governments to act proportionately in cyberspace and in accordance with national and international law; (2) The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity - to access cyberspace;
(3) The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas; (4) Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression; (5) The need to respect individual rights of privacy and to provide proper protection to intellectual property; (6) The need for the international community to work collectively to tackle the threat from criminals acting online; (7) The promotion of a competitive environment which ensures a fair return on investment in network, services and content.\textsuperscript{35} In practice, the British government has vigorously promoted the “London process” by holding cybersecurity conferences in London, Budapest and Seoul in succession to influence and even control the general direction of cybersecurity rule-making.

Eneken Tikk, a legal advisor at the NATO Cooperative Cyber Defense Centre of Excellence (CCD COE) put forward ten rules for cybersecurity in 2011, including the territoriality rule, the responsibility rule, the cooperation rule, the self-defense rule, the data protection rule, the duty of care rule, the early warning rule, the access to information rule, the criminality rule, and the mandate rule.\textsuperscript{36} On October 20, 2011, the Chinese ambassador for disarmament affairs Wang Qun proposed five principals in his speech at the first committee of the 66\textsuperscript{th} session of the UN General Assembly, namely, the principle of peace, the principle of sovereignty, the principle of balance between freedom and security in information flow, the principle of cooperation, and the principle of equitable development.\textsuperscript{37} Moreover, the World Economic Forum held in Davos, Switzerland in 2010 had a separate session named “Securing Cyberspace” to discuss the prospect of establishing an international framework or treaty to enhance cybersecurity. At the session, Hamadoun Touré, Secretary-General of the International Telecommunications Union (ITU) said that the risk of cyber conflicts between countries was growing every year, and that a treaty on cybersecurity would help prevent attacks on the cyber community from becoming an all-out war. The treaty, according to Mr. Touré, would look like a peace treaty before a war.\textsuperscript{38}


The aforementioned cybersecurity policy proposals are not only different in names, but also in content and emphasis. They actually reflect different interests and demands of various countries on the issue.

2. Different types of cybersecurity rules

Generally speaking, cybersecurity rules can be divided into four groups: general rules, cyber criminal rules, cyber-warfare rules and information technology rules. The general rules include cyberspace sovereignty, cyber freedom and cybersecurity (or control of the cyberspace), etc.

Cyberspace sovereignty is a natural extension of state sovereignty in cyberspace, which should be respected and safeguarded. Sovereign states are the main actors in maintaining order in cyberspace and the respect of cyberspace sovereignty is an important prerequisite of safeguarding cybersecurity. The public policy that a country has adopted for maintaining order and security in cyberspace should be respected. At present, many international organizations, including the UN and NATO, and quite a number of countries, such as the United States and China, have acknowledged the principle of cyberspace sovereignty and the jurisdiction of a sovereign state over cyber issues within its territory. That should serve as an important foundation for future global internet governance and cybersecurity enhancement.

Unlike the principle of cyberspace sovereignty, the principle of cyber freedom has triggered some disputes in the international community. Some countries are afraid of other countries intervening in their internal affairs and violating their sovereignty on the pretext of protecting cyber freedom. Generally speaking, western countries, such as the U.S. and the U.K., advocate free flow of information on the Internet, while Russia prioritizes information security and China supports free and secure flow of information.

The former U.S. Secretary of State Hillary Clinton is a staunch advocate of cyber freedom and an active practitioner of cyber diplomacy. In January 2010, she delivered a speech on internet freedom at the Newseum in Washington, in which she summarized the idea that governments should not prevent people from connecting

---

to the Internet, to websites, or to each other as “the freedom to connect”, and put it in parallel with the traditional four freedoms of the United States. In February 2011, Ms. Clinton made a speech at George Washington University, saying that “the United States supports the use of internet by civil society via its ‘2.0 Initiative’, which connects nongovernmental organizations and advocates with technology and training that supports their work”. She said that “the struggle for internet freedom is a struggle for human rights, human freedom and human dignity”. In practice, the United States attaches importance to publicizing U.S. foreign policy by making use of various information platforms, among which social media has become “a new arrow in its quiver”. However, the Snowden incident has exposed the dual character of U.S. policy on cyber freedom.

In fact, there is neither absolute cyber freedom nor absolute cybersecurity. The aforementioned general cyber rules have both universal applicability and certain relativity. In practice, every country need strive for balance among sovereignty, freedom and security.

Most cyber-attacks belong to cybercrime and currently they constitute the severest threat to cybersecurity. To address it, many countries have promulgated new laws, and the UN Commission on Crime Prevention and Criminal Justice has set up an intergovernmental expert group to conduct a comprehensive study of cybercrime and responses to it. At present, countries around the world have already carried out lots of cooperation in tackling cybercrime, but a universal treaty or law on cybercrime has not come into existence. Among existing international agreements on cybercrime, the Convention on Cybercrime (also called Budapest Convention on Cybercrime) adopted by the Committee of Ministers of the Council of Europe in 2001 is a comparatively complete one. However, it has also some problems, such as outdated contents and inadequate representativeness.

In the future, although cracking down on cybercrime by practical cooperation will continue to be an important part of the international efforts in enhancing cybersecurity and maintaining cyberspace order, the focus and the difficult part would be the formulation of universal laws and regulations on cybercrime. In drafting these laws and regulations, we need consider not only universal

41 The traditional four freedoms of the United States are the freedom of expression, the freedom to worship, the freedom from want, and the freedom from fear. See “Hillary Clinton's Speech About Internet Freedom”, January 21, 2010, http://www.hillaryclintonquarterly.com/hillaryclintonspeechinternetfreedom.htm.

applicability, but also concrete national conditions as well as historical and cultural backgrounds of various countries and regions.

The ICT rules and standards are the foundation of internet governance. Due to differences in the level of ICT development, countries around the world have different positions in global internet governance and the sharing of basic information resources. They have been competing with one another for internet administrative power and on such technological issues as the opening of source code. As to the making of ICT rules and standards, the authority of the ITU should be respected and brought into full play, and such organizations as the Internet Corporation for Assigned Names and Numbers (ICANN) should be more democratic.

C. Cyber-warfare and the rules for cyberspace arms control

The aforementioned Code of Conduct, Budapest Convention on Cybercrime, the Tallinn Manual and other proposals relating to cybersecurity could be used for reference in future international cyberspace legislation. Viewed from the international law standpoint, there is no universally applicable international treaty or legal document that covers all major aspects of cybersecurity or specially drafted for it, let alone international rules applicable to cyber-warfare and cyberspace arms control. The international community can regulate online activities of different types of actors by formulating international rules at different levels and in different forms, including among others a universally-binding treaty or an international agreement regulating acts of cyber war and cyber armament. However, the United States tries to legitimize its cyber-attacks through “pre-emptive cyberstrikes” policy, which is not only useless for cyberspace arms control and its rule-making, but could cause a series of problems.

1. Cyber-warfare and the international treaty

Compared to physical space, such as the land, the sea, the sky and the outer space, cyberspace has its uniqueness. Although the existence of cyber-warfare is still a controversial issue and many problems would emerge when we apply the existing international law to cyberspace, we should still explore the applicability of
the existing international law (including the law of war) to cyberspace.

In drafting the *Tallinn Manual*, NATO gathered dozens of experts on international law, international relations and cybersecurity from its member states, and the governments of these states sent their representatives to observe the discussions. As a guiding book, the *Tallinn Manual* is quite comprehensive in its contents. Of course, NATO said the *Tallinn Manual* did not represent its official position and that the views in it were only those of the authors. Considering that many people still doubt the existence of cyber-warfare, the publication of the *Tallinn Manual* shows that western countries have run ahead of other ones in exploring the norms of cyber-warfare.

As a matter of fact, cyber-warfare poses plenty of challenges to the existing international law, including invalidation of the traditional concepts of “territory” and “sovereignty”, the difficulty in finding out who is to blame for an international injury; inapplicability of the “legitimate self-defense” principle and the “declaration of war” principle, the problem of applying the principles of distinction and military necessity, the difficulty in defining legitimacy of cyber deception, and impossibility to protect the interests of neutral States. Therefore, the existing international law cannot be directly applied to cyberspace. For instance, Article 2, Chapter I of the UN Charter stipulates that “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations”. This article can be interpreted to have covered the acts of information war through the Internet, thereby determining the illegitimacy of such acts. However, it is not easy to identify the acts of information war and normally two countries go to information war unnoticed. This requires us to have a more detailed explanation of relevant rules to adapt to the reality of cyberspace so as to attain the goal of maintaining international peace and security.

The *Outer Space Treaty* stipulates that the Moon and other celestial bodies shall be used by all State Parties to the Treaty exclusively for peaceful purposes. However, satellites could serve as the relay platform in cyber war, and the Treaty does not ban such use of the satellites. The *Constitution of the International Telecommunication Union* provides that “all [radio] stations, whatever their purpose, must be established and operated in such a manner as not to cause

---

harmful interference to the radio services or communications of other Member States...”. However, the cyber weapons under development could not only cause harmful interference to the radio services of other Member States, but change the information in transmission, which obviously go against the purposes of the Constitution. In addition, the OECD Guidelines for Security of Information Systems adopted in 1992 only relates to computer crimes and not to the information war.

Rich in contents, the aforementioned Code of Conduct aims at limiting the non-peaceful use of the Internet and internationalizing internet governance. However, the United States holds the view that the existing international framework is adequate for curbing cyber-attacks because it fears that China and other nations might use all possible means (including international public opinions and new international conventions) to limit U.S. military choice. Moreover, the United States insists that the technical difficulties in attribution, inspection and others would seriously affect the credibility and effectiveness of any international treaty for cyberspace arms control. The truth is that the United States wants to make it an excuse for maintaining its supremacy and technological advantages in cyberspace.

As mentioned earlier in this chapter, information security has been on the UN agenda and there have been annual reports by the UN Secretary-General to the General Assembly on the issue since Russia submitted its proposal to the UN for the first time in 1998. In addition, the United Nations has set up three groups of government experts (GGE) to examine the existing and potential cyber threats and put forward possible cooperation measures to address these threats. On the basis of the 2010 GGE report (A/65/201), the third Working Group submitted a new report (A/68/98) in June 2013. Compared to the first report, the new one made a lot of progress. For example, in the part “Recommendations on norms, rules and principles of responsible behavior by States”, the new report states,

“The Group noted document A/66/359, circulated by the Secretary-General at the request of the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, containing a draft international code of conduct for information security. ... International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open,
secure, peaceful and accessible ICT environment. ... State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory”.

Besides, the new report contains important consensus reached in such aspects as confidence building measures and ICT capacity building measures for developing countries.45

Actually, the new report of the GGE is both the result of negotiation and compromise among various countries and a fruit of their practical cooperation. With progress in both general principles and concrete issues, it opens a window of opportunity to discuss the applicability of the international law to cyberspace and provides a foundation for future international agreement on cybersecurity. In the coming years, the international community should probe for ways to apply the existing international law to the new reality of cyberspace and the possibility of creating new legal provisions in accordance with the new reality, thereby enhancing legitimacy, applicability and effectiveness of the international law.

2. Cyber-warfare and the principles of armed conflict

Although the law of armed conflict (LOAC) has the most direct bearing with cyber-warfare, it can only be applied to the situation in which two countries have armed conflict from the international law perspective. According to the Geneva Convention, “belligerence” refers to physical confrontation, and “entering the territory of another country” means border-crossing. The current LOAC only involves land, sea and air battles, and cyber-warfare does not belong to any of them. In cyber war, there is neither physical damage as bad as an explosion nor tangible territory seizure by military forces, and because of that, applying the LOAC to cyberspace become a very controversial issue. Currently, most people believe that the LOAC can be applied to cyberspace only under two circumstances: first, countries are in a state of war; second, the damage caused by cyber-attacks has reached a level comparable to that of a real war, especially inflicting direct large-scale casualties.

The principles of armed conflict are the code of conduct that combatant parties should abide by, including: (1) the principle of military necessity. The combatant parties can only use the regular military forces permitted by the LOAC, with the minimum price, to partly or completely subdue their enemies. Since the targets in cyber war are usually critical infrastructure, the damage to which could easily lead to paralysis of a society, the use of such cyber weapons would be far beyond “military necessity”; (2) the principle of humanitarianism. The means of warfare must be corresponding to the purpose of the war. The current LOAC limits the use of such weapons as landmines and napalm bombs, but not cyber weapons, such as “computer viruses” and “logic bombs”. Although the latter’s destructive power is in no way smaller than the former, they are not covered by the existing LOAC; (3) the principle of knighthood. This principle stresses that the combatant parties must have “complete formalities” before launching attacks. The LOAC permits the use of deception. However, if one party issues the order of laying down arms to its adversary’s soldiers in the name of their highest commander, the adversary probably would suffer heavy losses. That was partly demonstrated by the Iraq War. Although at that time they were just slogans to induce capitulation, which belongs to psychological warfare and propaganda campaign, the destructive power of cyber weapons had been well displayed. A key question for future discussions is how to make the principles of LOAC fit such phenomena.

An expert at the Washington-based Center for Strategic and International Studies (CSIS) believes that the current LOAC can be applied to cyberspace, and its principles, such as proportionality and distinction, have already provided the basis for protecting civilians. This view is correct in a broad sense. For example, although the line between civilian and military infrastructures is blurred, the Geneva Convention of 1949 and the Hague Conventions of 1899 and 1907 all include rules on protecting civilians, and all countries should abide by these rules in cyberspace as well. However, in applying the principle of distinction, the first difficulty might be how to distinguish civilian and military networks. Different from other physical infrastructure, civilian and military networks are very hard to distinguish from one another. Even for those civilian or military networks physically isolated from the Internet, the so-called “off-line bombs” and “logic bombs” can penetrate into them and cause damage. In addition, the threshold of defining a cyber activity as an attack should be high because not every evil deed
in cyberspace is an attack or use of force, and most spiteful activities in it do not constitute acts of cyber war. Otherwise, countries around the world would fall into the Hobbesian war of everyone against everyone.

In a word, the spirit of the law of war can be applied to cyberspace, but the specific articles and provisions should be adjusted in accordance with the characteristics of cyberspace. It is meaningless to talk about the applicability of the law of war in cyberspace in abstract terms.

3. “Preemptive” cyberstrike policy goes against the trend

Whether as a sign of U.S. attitude toward cyber-warfare or as a tentative move, or out of its self-conceitedness, the aforementioned secret legal review on the use of U.S. growing arsenal of cyber weapons concludes that President Obama has the broad power to order a preemptive strike if the United States detects credible evidence of a major digital attack. In fact, the U.S. has always been striving for dominance in exploring and formulating cyberspace rules. Apart from vigorously advocating cyber freedom, the United States has tried to use its preemptive cyberstrike policy as a touchstone for formulating cyber-warfare rules and to promote the application of the law of war in cyberspace from the opposite direction. The U.S. move also aims at providing legitimacy for its cyber-attacks, though such self-granted legitimacy has no basis in the international law at all. Moreover, the preemptive cyberstrike policy faces an inherent dilemma - those countries subject to U.S. preemptive cyberstrikes can easily argue that they are innocent, and if the United States cannot provide credible evidence, the legitimacy of its preemptive policy will be lost. Even a U.S. senior official admitted, “It would be very hard to provide evidence to the world that you hit some deadly dangerous computer code”.

In making new rules, the United States is not free of misgivings. Actually it has paid a great deal of attention to the impact of its preemptive cyberstrike policy. According to a U.S. official involved in the secret legal review, one major issue in the review is defining “what constitutes reasonable and proportionate force” in halting or retaliating for a cyber-attack. The U.S. is particularly worried about its preemptive cyberstrikes becoming an excuse for other countries to launch cyber-

---

attacks on it, thereby threatening its national security. For instance, during the U.S. cyberstrike on Iran’s nuclear facilities (the U.S. has never admitted it), President Obama insisted on “accurately positioning” and not affecting the operation of hospitals and electricity supply in Iran. He had repeatedly shown his worry that other countries might use this incident as a pretext to launch cyber-attacks on the United States. Herbert S. Lin, a cyber expert with the U.S. National Academy of Sciences said,

“We are having a big debate about what constitutes the use of force or an armed attack in cyberspace. We need to know where those lines are so that we don’t cross them ourselves when we conduct offensive actions in cyberspace against other nations.”

In fact, the secret legal review was made to solve legal problems faced by the U.S. preemptive cyberstrike policy. As it is, this policy has basically delineated the boundaries of “legitimate” U.S. cyber offensive actions, and paved the way for future American preemptive cyber-strikes. However, the problem here is when the United States is pursuing its security through preemptive cyberstrike policy, other counties become less secure and their sense of fear and being threatened will only increase. To enhance their cybersecurity, those countries might have to strengthen their cyber arms, and a cyber arms race may be triggered, which is apparently not conducive to promoting cyberspace arms control, safeguarding cybersecurity and constructing a good order in cyberspace.

---

V. Cyberspace Arms Control and Sino-American Cyber Relations

The United States, as the largest developed country in the world, is much more advanced in information and communications technology (ICT) than any other country, while China, the biggest developing country across the globe, has the largest number of internet users. Cyberspace has inevitably become a new field for the two countries to make contact and develop relations. Actually, recent years have witnessed the development of Sino-American cyber relations into both an important part of the bilateral ties and a key variable affecting other aspects of the bilateral relations.

A. The development of the Internet and the cybersecurity situations in China

The Information Office of the State Council, or China’s cabinet, issued a white paper on the Internet in China on June 8, 2010, which says:

“China takes Internet development as a significant opportunity to boost its reform and opening-up policies and modernization drive. The government has worked out a series of policies for Internet development, defining the phased priorities to boost information technology application across the country.”

The year 2014 marks the 20th anniversary of China’s formal access to the Internet. During the past 20 years, the Internet in China has developed rapidly and now the Internet has become an indispensable part of Chinese people’s daily life. According to the 33rd Statistical Report on Internet Development in China released
by China Internet Network Information Center (CNNIC) in January 2014, China had 618 million internet users by the end of 2013 and the internet penetration rate was 45.8%. By the same time, China had 500 million mobile internet users and the rural internet users accounted for 28.6% of the total, reaching 177 million. There were totally 18.44 million domain names in China, among which the .CN domain names were 10.83 million, accounting for 58.7% of the total. By the end of 2013, China had 3.2 million websites. From these statistics we can conclude that the Internet in China has developed swiftly and its application is quite extensive.

However, at the same time, China is faced with many cyber threats, and safeguarding its cybersecurity is a challenge that cannot be neglected. According to “A Summary of China’s Cybersecurity Situation in 2013 – Viewpoints of the CNCERT” released by the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT) in March 2014, the operation of China’s basic information network was generally stable, but the domain names system remained vulnerable in 2013. Although initial success had been achieved in public internet governance, cracking down on the underground industrial chain of hackers was still an arduous task. And the mobile internet environment had deteriorated and the problem of pollution in cyberspace should be solved without delay. Moreover, China’s economic information security faced more threats, and information consumption was confronted with cross-platform risks. What should be noticed in particular was that an increasing number of state-sponsored organized cyber-attacks posed severe threats and challenges to China’s critical infrastructure and important information systems. According to the monitoring of the CNCERT, China currently faces a large number of cyber offensive actions from overseas addresses, such as backdoors, phishing, Trojans and Botnets.

Besides formulating a series of policies to promote internet development, China has gradually included the issue of cybersecurity into its national political agenda, and used multiple means, including legislation and institutional setup, to safeguard its cybersecurity. On February 27, 2014, the first meeting of the Central Leading Group on Internet Security and Informatization (CLGISI) was held in Beijing. In his speech, President Xi Jinping stressed that internet security

---


and informatization were major strategic issues relating to national security and development as well as the work and life of the masses, and that we should start from the general international and domestic trends, make an overall arrangement and integrated efforts, promote development through innovation so as to build our country into a cyber power. President Xi described internet security and informatization as “two wings of a bird and two wheels of an engine”, and said that we must integrate our planning and arrangements, and make coordinated efforts in boosting internet security and informatization. “To do a good job in both aspects”, Xi said, “we should well handle the relationship between security and development, coordinate our efforts and advance our work together.” He stressed that we ought to safeguard development with security and promote security through development so as to achieve long-term security and stability, and that there would be no national security without cybersecurity, and no modernization without informatization. President Xi stressed that in the future, the CLGISI would play the role of centralized and unified leadership, plan as a whole and coordinate the efforts made to address major issues relating to internet security and informatization in all fields, and formulate and implement national strategy, grand plans and major policies on the two aspects in order to strengthen China’s capacity in safeguarding its security.\textsuperscript{51}

**B. Viewing cyberspace arms control from the angle of Sino-American cyber relations**

As mentioned earlier, with many countries speeding up their cyber army building, China faces mounting pressure in safeguarding its cybersecurity, and cyber issues have increasingly obvious impact on China’s foreign relations. For instance, from January 2013 to August 2013, more than 20,000 websites based in China were modified by hackers and over 8 million servers were compromised and controlled by overseas computers via zombie and Trojan programs. More than 80 percent of Chinese internet users have fallen victim to cyber-attacks and the annual economic losses run to tens of billions of U.S. dollars a year.\textsuperscript{52} With its monitoring


\textsuperscript{52} Speech by Minister Cai Mingzhao at Cyber Summit 2013, November 5, 2013, Transpacific, http://transpacific.net/2013/11/05/full-text-speech-by-minister-cai-mingzhao-at-cybersummit2013-nov-5-2013/
power of the root servers for domain names and its monopoly in computer hardware and software, the United States has a firm control of the Internet. However, due to its heavy reliance on the Internet, the country is also vulnerable to cyber-attacks.\footnote{《美国政府网络面临极大挑战，封闭只会导致灾难》[“U.S. Government Network Is Facing Severe Challenges and Closure Will Only Lead to Disaster”], 中国计算机安全网[China Computer Security Network], October 8, 2012, http://www.infosec.org.cn/news/news_view.php?newsid=16271.} Facing common challenges and threats, China and the United States should strengthen exchanges and communications in the field of cyberspace arms control and take the lead to establish standards and principles, and to explore ways of action in the field, while striving to enhance their own capabilities in cyberspace.

1. **Setting up priorities for cyberspace arms control and focusing on regulation of state-sponsored online behaviors**

   The cyber-warfare is usually divided into two levels. The first one is “strategic cyber-warfare”, which is mainly fought on the Internet with the purpose of paralyzing state apparatus and bringing about social unrest and the downfall of enemy countries’ governments by attacking their political, economic and military networks. The second one is “cyber-warfare on the battlefield”, which mainly refers to offensive and defensive actions in the wired or wireless networks on the battlefield with the aim of destroying enemies’ command, control, intelligence and reconnaissance systems. To prepare for the second-level cyber-warfare has been an important direction of major countries’ army building since the end of the Cold War.

   The cyberspace arms control aims at preventing strategic cyber-warfare mainly. As said before, during a strategic cyber war, countries exploit information technologies to attack the computer systems indispensable for the operation of enemy countries’ political, economic and military organizations and facilities as well as their social systems. The goal of cyber-attacks in a strategic cyber war is to paralyze the enemy’s military, financial, power supply and transportation systems. Once these critical infrastructures were attacked, loss of water and electricity, traffic tie-up and strategic weapons getting out of control would have happened one after another. The United States is trying to use multiple means in a comprehensive manner to protect its critical infrastructure against cyber-attacks, including restricting state-sponsored offensive actions by negotiating multilateral agreements. In view of that, future cyberspace arms control should focus on state-sponsored
cyber-attacks.

2. The United States intends to dominate cyberspace arms control and China should actively participate in the process

As commented by the Financial Times, the International Strategy for Cyberspace announced by the White House in May 2011, for the first time, unified U.S. international goals for internet policy.\(^\text{54}\) Upon the release of the strategy, U.S. Secretary of State Hillary Clinton said that the strategy identified seven key policy priorities that would be the focus of U.S. diplomatic outreach going forward, and that these seven priorities comprise a new foreign policy imperative for which U.S. State Department had been exercising and will continue to have a leading role.\(^\text{55}\)

In the future, the United States will continue to publicize and implement its internet strategy via diplomacy and other supplementary means, through bilateral and multilateral channels, so as to set the global agenda on internet development, governance, freedom and security, and dominate the making of rules and standards on global internet development and security. Having different views with the United States on many cyber issues, including cyberspace sovereignty, internet freedom and cybersecurity, China should be more active in participating in the making of cyberspace rules and take the initiative to raise relevant proposals so as to have a greater say on cyber issues.

3. The United States has a relatively well-developed legal system on cyber issues and China can draw on its experience

With its superiority in ICTs, the United States will continue urging developing countries to further open their markets for information and network technologies as well as IT products and services. To list the U.S.-defined hackers as wanted and crack down on cybercrime, the United States will seek coordination with other


\(^{55}\) The seven policy priorities are: (1) Economic engagement to encourage innovation and trade while safeguarding intellectual property; (2) Cybersecurity to protect U.S. networks and strengthen international security; (3) Law enforcement to improve U.S. ability to respond to cybercrime; (4) Military cooperation to help U.S. alliances do more together to confront cyber threats while ensuring that U.S. military’s networks remain protected; (5) Multi-stakeholder internet governance so that networks work the way they should; (6) Development to support the rise of new partners by helping countries develop their digital infrastructure and build their capacity to withstand cyber threats; (7) Internet freedom. See “Secretary Clinton on U.S. International Strategy for Cyberspace”, IIP Digital, May 16, 2011, http://iipdigital.usembassy.gov/st/english/texttrans/2011/05/20110516180150su0.9489819.html#axzz34PNg395i.
countries in the fields of cyber law enforcement and cyberspace justice, which would facilitate cross-border enforcement of U.S. cyber laws.

The United States has a relatively well-developed legal system on cyber issues, and its domestic cyber laws will have great influence on international arms control in cyberspace.

As the first country to adopt information policy with legal effect in the world, the United States started doing that in the 1950s. With wide application of computers and the Internet, a series of laws and policies have been promulgated from the 1970s to the 1990s. The laws and policies released in this period have strong professional and technical characteristics and the contents mainly relate to computer communications security and privacy protection. Since the 1990s, the newly adopted U.S. cyber policies have included increasingly more contents other than the technical ones. For instance, the National Information Infrastructure: Agenda for Action (also known as the Information Highway Strategy) released in 1993 marked the beginning of U.S. informatization efforts. In 1995, the U.S. National Telecommunication & Information Administration (NTIA) issued a report entitled “The Global Information Infrastructure: Agenda for Cooperation”, the purpose of which was to amplify the five principles proposed by U.S. Vice President Al Gore at the first World Telecommunication Development Conference in 1994 and to identify the steps the United States, in concert with other nations, could take to make the vision of the Global Information Infrastructure (GII) a reality.

Since the start of the 21st century, the United States has further accelerated its cyber legislation and given more consideration to such factors as national

---


57 The five principles are: first, encouraging private sector investment; second, promoting cooperation, third, providing open access to the network for all information providers and users; fourth, creating a flexible regulatory environment that can keep pace with rapid technological and market changes; and finally, ensuring universal service. See The Global Information Infrastructure: Agenda for Cooperation, June 1, 1995, http://www.ntia.doc.gov/report/1995/global-information-infrastructure-agenda-cooperation.

58 In addition, the plan for “next generation of Internet” unveiled in 1996 aimed at maintaining U.S. supremacy in ICTs and U.S. leadership in world economy and politics by updating its computer systems more frequently so as to solve the existing systems’ problems, such as obsolete equipment and overloading. The Internet2 Project formally established in 1997 provides the U.S. research and education community with a network that satisfies their bandwidth-intensive requirements and promotes the development of higher education and information service provision worldwide.

The U.S. cyber legislation has not only started early, but covered many aspects, including technology, politics and international relations. In its own cyber legislation, China has already drawn on the U.S. experience. And the cooperation between the two countries on cyber legislation has been conducted to some extent. However, there is no in-depth and systematic study on U.S. cyber legislation in China yet. Apart from deepening its research on U.S. cyber legislation, China should strengthen communication with the United States and clearly state its positions on cyber issues so that the international rules on cyberspace arms control can be formulated at an early date.

4. China and the United States should cooperate in exploring possible plans for cyberspace arms control

For years, the United States has objected to the proposal of establishing a treaty for arms control in cyberspace for fear that strict global regulation of cyberspace would hinder innovations and affect an essential feature of cyberspace - openness, thereby weakening the dominant position of American network companies in the IT field. However, due to its heavy reliance on computers and computer networks, the United States has become one of the most vulnerable countries to cyber-attacks. Keith Alexander, the Commander of U.S. Cyber Command, once said that what Russia had put forward was, perhaps, the starting point for international debate, and that it was something that the United States should, and probably would carefully consider. However, Gen. Alexander didn’t think cyber disarmament could be done


in the same way with the U.S.-Russia Strategic Arms Reduction Treaty (START) because nuclear warheads and missiles could be counted and traced, whereas cyber weapons were like biological weapons, which could be used at any time. Therefore, China should be well aware of U.S. major concerns on cyberspace arms control.

Generally speaking, the answers to the following three questions will determine U.S. willingness to participate in cyberspace arms control: First, can U.S. infrastructure stand state-backed cyber-attacks? Second, does the United States have reliable cyber-warfare capability to launch strategic strikes on other countries’ infrastructure? Third, does a normative international treaty only have sense in preventing the United States from developing cyber weapons or can other countries ensure the fulfillment of their commitments specified in the treaty? Considering the importance of cyber offensive and defensive capabilities in military actions and the deterrent role they play, it is unlikely that the United States will agree to any provisions that would hinder the development of its cyber-warfare capabilities. As a matter of fact, the United States stressed that as part of its infrastructure protection strategy, it would use the Internet to prevent cyber-attacks on its infrastructure.

Since mid-1990s, the U.S. government has been taking various measures to enhance the security of its critical infrastructure, which include upgrading security programs and technologies of its computer system, adopting new standards and norms and more importantly, seeking improvement measures from American citizens. Three U.S. presidents in succession, Bill Clinton, George W. Bush and Barack Obama have all announced their work programs on the enhancement of infrastructure security, and apart from government agencies, influential companies, trade associations and research institutes in the United States have also participated in the work programs. However, the only conclusion is that the United States has not made remarkable progress in cybersecurity enhancement, and no one can answer the following question - does the United States have the capability to effectively strike other countries’ infrastructure with cyber weapons? For the above reasons, the United States can hardly reject the proposal of negotiating an international cybersecurity treaty, which would set limits on the development of other nations’ cyber-warfare capabilities.

In the future, China and the United States should conduct cooperation to explore possible plans for cyberspace arms control.
5. Promoting multilateral cooperation and global internet governance

Just like in many other fields of international relations, the stances of China and Russia on cyber issues are distinct from that of the United States, and that has become an excuse for the latter to make cyber war preparations. The U.S. National Intelligence Council pointed out in 2009 that globally China posed a complex threat to the United States and the former might launch cyber-attacks on the latter.

As for cyberspace arms control, China and Russia have more common understandings with other developing countries compared with the United States. Besides the aforementioned *Code of Conduct*, the Shanghai Cooperation Organization (SCO) adopted the *Statement of Heads of Member States of SCO on International Information Security* in June 2006. Moreover, China and Russia have respectively conducted self-contained research on information security. The two countries are more concerned about information security, which is a broader concept than cybersecurity, while the United States focuses its attention on the latter. Therefore, in negotiating an international agreement on cybersecurity and cyberspace arms control, China should strengthen its communication and coordination with Russia and other like-minded countries.

Despite its obvious advantage in the internet field, the United States cannot dominate the making of rules and policies in cyberspace globally. The ITU and other UN organs will continue to be important places for international negotiation on cyber issues. Both China and the United States should lend full support to the UN and its entities and work together to establish a transparent multilateral distribution system of the Internet’s basic resources so that every country can have an equal right in managing these resources and the Internet can develop in a balanced way worldwide. By doing that, the two countries will not only safeguard their own cybersecurity, but contribute to the enhancement of global cybersecurity and internet development.
Conclusion

The rapid development of information technology has changed people’s way of life, the connotations and denotations of the concept “national security”, and basic forms of modern warfare. In the past, we can only conquer a country by capturing its territories with military troops, whereas at present we can damage a country’s infrastructure and affect its people’s normal life with cyber-attacks. Cyberspace is evolving into a new battlefield and a new place to commit crimes. The international community, especially China and the United States – the two major powers - must make concerted efforts in establishing rules and treaties to regulate cyber activities. Since the two countries are both vulnerable to cyber-attacks, and cyber threats are their common challenges, cyberspace arms control can be a field in which the two countries test the idea of building a new type of major-power relationship.

In practice, the international law and rules always fall behind the technological development. With rapid development of the information technology, the soft-kill capacity of such technology needs to be regulated and restrained. And how to achieve that is an issue that the international community need think over and seriously address, though such capacity features no physical damage.

The present cyberspace is like the newly built highway in the 20th century when the automobile industry was just flourishing. At that time, those who had good cars could drive at their will on highways because the traffic rules for highways had not been made yet. Likewise, those countries with advanced information technology now can do whatever they want in cyberspace because the rules for cyberspace have not been established yet. However, with the spread of information technology, an increasing number of countries will possess and apply this technology. In addition, the characteristics of information technology enable common citizens to act as cyber warriors, inflicting catastrophic damage on countries.

As the most advanced country in information technology, the United States is reluctant to talk about “cyberspace sovereignty” or strategic cybersecurity. What
it is willing to discuss is cybercrime, which is closely related to U.S. interests. Compared with the nuclear technology that the United States tried to monopolize when it was emerging, the information technology can be spread faster and
popularized easier, hence impossible for the U.S. to monopolize it. The Internet
is interconnected and vulnerable to attacks, therefore it is necessary for the
international community to make joint efforts in maintaining its order, which makes
a new demand for cyberspace arms control.

Currently, China and the United States are working toward the establishment
of a new type of major-power relationship, and cybersecurity is an issue to which
both nations have paid close attention. To enhance the bilateral cooperation in
cybersecurity, the two countries should, first of all, be aware of the differences of
their major concerns on the issue and build consensus on that. Only by doing that
can they have effective communication. Secondly, the China-U.S. dialogues on
cybersecurity should focus on their common demands, not repeatedly calling the
other side to account. Finally, cybersecurity is not an issue of China and the United
State only. Recognizing the spread of cyber technologies cannot be limited by
traditional boundaries, China and the United States need join hands with all other
countries to address the problem. The two nations should shoulder major powers’
responsibilities by formulating rules to regulate the activities in cyberspace so that
human civilization can sustain and develop in an orderly way in the fifth space
following its development on the land, in the sea, the air and the outer space.

(This report is translated by Zhu Hongtao, Huo Yan and Xue Fei, and proofread
by Wang Qiang.)
Cyber War Preparedness, Cyberspace Arms Control and the United States

Treaty Could Help Prevent Cyber Wars,

US can trace cyber attacks, mount pre-emptive strikes, Panetta says,

Russia’s Cyber Force,
List of Published CIIS Reports


About the Authors

Teng Jianqun is a senior research fellow at China Institute of International Studies (CIIS). He is also director of Center for Arms Control and International Security and director of Department for American Studies, CIIS. Mr. Teng joined the CIIS in 2004 after being discharged from active military service. He had served in the PLA for 25 years, first in the Navy (1979-1992) as a military officer and later in the Academy of Military Science (1992-2004) as an editor of World Military Review, an academic journal run by China Association of Military Science and the Academy of Military Science. Mr. Teng has authored several books and reports, and published hundreds of articles on such issues as international arms control and disarmament, theories of international security, and American military strategy. He has accomplished a National Social Science Fund (NSSF) project entitled “On Arms Control and Disarmament Issues” and is going to finish another NSSF project “The PRC’s Arms Control and Disarmament History”. Mr. Teng holds a doctorate in international relations, obtained from Peking University in 2006.

Xu Longdi is an associate research fellow at Department for European Studies, CIIS. His main research fields include theories of international relations, international security, cybersecurity, and European politics and foreign policy. Mr. Xu joined the CIIS in 2009 after graduation from Graduate School of Chinese Academy of Social Sciences (CASS) with a doctorate in international relations.
ABSTRACT

This report presents first of all the general situation of current cyberspace, and then it introduces discussions on cyber-warfare in the international community and the restraints on cyber-warfare imposed by the existing international law as well as other issues. Subsequently, it analyzes cyber war preparedness and demands for cybersecurity of the United States and other countries. Finally, it proposes that a new regime and a new set of rules for cyberspace arms control be established so as to avoid the abuse of cyberspace and not to trigger international conflicts, for which the United States has unshirkable responsibility. The report holds that as China and the United States are working toward the establishment of a new type of major-power relationship, cooperation in cyberspace should be an important part of that endeavor.