The Study on the Situation, Security Challenges and Construction of a Community of Shared Future in Global Cyberspace

Zhi LI

Ningbo Institute of Technology, Zhejiang University, Ningbo, Zhejiang, 315000, China

Keywords: Community, Global Cyberspace, Security Challenges, Construction

Abstract. As an important part of the Socialism with Chinese Characteristics for a New Era, and one of the basic strategies for nation building. The call for a community of shared future for mankind on the world stage has gradually been recognized by the international community. Today, the Internet has connected the vast world into a small "global village." Under the impact and penetration of the global network wave, the increasingly prominent cyber security problem has caused major economic losses to the security of network core facilities in the world, and it has become a worldwide problem. China, as a large network country, actively advocates building a community of shared future in cyberspace, contributing China's wisdom and solving world network problems. It is not only the need of the country's own construction, but also the responsibility and mission of the new era to assume the great power of the new era, and it is conducive to strengthening the international community. The construction of communication capabilities will explain the image of China to the world and enhance its international influence.

With the widespread penetration of the Internet, cyberspace has now become the fifth space beyond land, sea, air, and the universe. Through the deep integration of virtual space and real world, more and more people are carrying social activities, while various known and unknown cyber security risks keep emerging, which has attracted global attention and even become the main topic of internet global governance. Then, how to find the key for a community of shared future in cyberspace is a common consensus in the international community. In particular, the "four principles" and "five propositions" advocated by President Xi Jinping at the world Internet conference have been widely recognized by the world. They respect cyber sovereignty, carry forward the spirit of partnership and cooperation, jointly safeguard and govern cyber security, and jointly build a community of Shared future in cyberspace.

1. Analysis of the Situation of Global Network Security

In recent years, information leakage has occurred frequently in the global network environment, and the scope and impact of information leakage have been escalating. According to the "Global Data Leakage Cost Study 2017" the global data reveal that cost research report, the total global 419 samples, the data reveal that the total cost of $14.1 billion on average, increased by 1.8% than normal size, whether government agency or organization enterprise, informatization level, the more developed countries, some large-scale data reveal that cause the more serious (IBM Security, 2017). Its contents involve frequent exposure of private events such as payment information, harassment information, life and financial information. It can be seen that the losses caused by information leakage are not only limited to the economic aspect, but also involve personal privacy, and even have an impact on the stability of social order, which is very worrying to all countries in the world. Combined with the specific situation of global network security, it is mainly reflected in four aspects: cyber security threat, cyber war conflict, cyber terrorism and cyber hegemonism.

First of all, the threat of cyber security is increasingly serious, and the government's core departments are still the main targets of cyber attacks. At present, the number of global cyber attacks continues to increase, and the frequency of attacks is on the rise. Such as, international hacking organizations such as “Anonymous” and “Lulz Security” have been highly intrusive in recent years, often targeting government agencies, financial organizations, and health departments,
including the invasion of the US CIA and Sony Corporation of Japan. Media tycoon Murdoch's TV station (Pei Tong, 2013). As early as in the 2012 Global Risk World Economic Forum, cyber attacks by governments and commercial organizations have been included in one of the five major threats to global stability (Huan Qiu, 2009).

Secondly, cyber warfare has become an important part of modern warfare. From the national level analysis, the intention of preparing for "cyber warfare" became more and more obvious. The network security company McAfee released a research report in November 2009, "In the immediate future: the era of network wars." Large countries such as the United States and France are accumulating website weapons, smashing espionage activities, using the network to control wars, and guarding against the outbreak of cyber warfare (Cheng Gong, 2014). Looking at the form of international cyber warfare, the United States is in a dominant position in cyber warfare because it controls most of the facilities of the global Internet, relying on strong hardware and software strength, and dare to start firstly.

Thirdly, cyber terrorism has also spread, and the Internet has become the main battlefield for terrorists to declare war. Terrorist organizations use the Internet to collect a large amount of information from governments, use the Internet to collect money and get rid of the original mode of exchange and donation, and develop towards intelligence to obtain political, military and economic information about the country. In particular, the popularity of new media has set off a new wave of cyber terror and provided convenient conditions for cyber terrorism. In addition, since the outbreak of the "Prism Gate" incident in the United States, the global panic has confirmed that the United States has absolute control over information in the field of network information security. The formation of cyber hegemonism has prompted countries around the world to pay more attention to cyber security issues.

Therefore, the development of global cyber security is not optimistic, has evolved into a strategic issue of the world, and has stimulated the evolution of international social form and competition. Although more and more countries have raised their cyber security issues to the national strategic level, they are also fighting for the control of information in cyberspace, consolidating the right to develop cyberspace, protecting the privacy of Internet users, combating international cybercrime, and preventing cyberspace breaches. Other issues have started a series of discussions and collaborations, but the results are minimal. However, fortunately, the construction of a global cyberspace community advocated by the Chinese government in recent years has received more and more attention and recognition from all over the world. It has launched a network security cooperation conference, established corresponding institutions, and strengthened network security construction. The foundation of the global cyber security destiny community has laid the foundation.

2. The Security Challenge of A Community of Shared Future in Cyberspace

First, ubiquitous. Cyberspace is the primary stage of the development of the Internet of things. It is a kind of widespread Internet space with ubiquitous characteristics. The community of shared future in cyberspace relies on the Internet of things to break the barrier between time and space to a certain extent. Members can access the Internet at any time through various terminal platforms. At the same time, under the condition of high coverage of network information, information can be widely spread throughout the world, in various fields, in various industries and among various departments through the network. This ubiquity provides great convenience to members, but it also has great hidden dangerous.

Second, data security. In the software (human) aspect, the ubiquitous nature means the diversity of community members. Different members have differences in technology application ability and data security awareness, which leads to differences in data protection awareness. In terms of hardware (materials), the ubiquitous nature means that the types of participating nodes are diverse, and the location distribution is uncontrollable, resulting in diversification and inferiority of data. Both of these aspects will lead to cyberspace data security issues.

Third, digital divide. Originally proposed by the NTIA (National Telecommunications and
Information Administration) in 1999, it refers to a gap between those who have tools in the information age and those who have not. In a community of shared future in cyberspace, different regions, countries, and races jointly build the same Internet, but the emergence of the digital divide due to differences in geography, culture, concepts, and languages has further triggered the Taylor effect of regions, countries, and races in the community. Causes security issues such as barriers and even conflicts in the network environment.

Fourth, wisdom. With the maturity of data volume, computing power and algorithms, artificial intelligence and deep learning are well known to the public. A community of shared future in cyberspace is built on a global network, including culture, economies, politics and many other aspects. It also means that a community of shared future in cyberspace is producing massive amounts of data at all times, based on distributed cloud computing and mature algorithms, while having intelligent features. The Artificial Intelligence Black Paper published by the 2018 World Artificial Intelligence Conference pointed out that artificial intelligence has six types of security risks: network security, data security, algorithm security, information security, social security and national security. It can be concluded that the five types of security risks are in wisdom. The same exists in the Internet space, and even the security risks are even more serious.

### 3. The Construction of a Community of Shared Future in Global Cyberspace

The construction of a community of shared future in global cyberspace is a long process, how has global cyberspace been managed. At present, the main body of the construction is diversified, including the state, social organizations, online media, opinion leaders, and netizens. The goal is to actively participate in the allocation of information resources, public opinion guidance, and order maintenance through the active participation of the main body, effectively solve the problems of information imbalance, public opinion crisis, disorder of order, etc., and jointly create freedom and equality in cyberspace. Continue to maintain a stable and healthy development network. The theoretical basis of the construction is based on the "a community of shared future for human" and based on the "five adherences" of China's new cosmopolitanism, and actively advocates a multilateral, democratic and transparent global network security governance system. That is, "persisting against hegemonism and Western centralism, advocating world multi-polarization and cultural pluralism; persisting in opposing regional protectionism, advocating free flow of people, money, goods and information, open cooperation; persisting in opposing self-interest and advocating for business Co-construction, win-win sharing, symbiosis and common prosperity; persist in opposing interference in other countries' internal affairs, advocate harmonious and inclusive, market operation, and peaceful development; persist in opposing denial, distortion, and tampering with history, and advocate keeping in mind history and preventing historical tragedies from repeating themselves(¥Peiren Shao, Junwei Wang,2018). The foundation of the construction is that China has already adopted the concept of network security innovation governance, bridging the digital divide, carrying out multilateral international cooperation, and making positive contributions to the international rules and network governance mechanisms of global cyberspace security.

(1) Hold to the new world theory and promote the establishment of a community of Shared future for global cyber security. Specifically, it protects the critical infrastructure and information security of the global network, maintains the order of the world's cyberspace, eliminates the digital divide, and advocates joint construction; Accelerate the pace of network facilities construction, encourage Internet technology innovation, and promote the sharing of global resources for the Internet. Fight against cybercrime and terrorist activities in accordance with the law, oppose cyber hegemonism, and advocate the diversified development of global network culture; Actively carry out international cooperation on cybersecurity, respect national sine sovereignty, protect personal privacy and intellectual property rights, achieve global network governance, and guarantee human rights equality. Therefore, the main body of the construction of cyberspace is a multivariate and jointly participated virtual space, which has become an indispensable part of the common destiny of mankind. Therefore, it is of practical significance to advocate a multi-polarization of the world, jointly build a multivariate
and cooperative global network security governance mechanism, and promote the construction of a community of shared future in cyberspace to benefit mankind.

(2) The principle that the bottom line is fair, open and cooperative, democratic participation, sovereign equality, legal order and data security are the principles of internet global security governance is a concrete manifestation of the "five tenets" of the new world doctrine. From the perspective of the internet global security governance environment, the development of global network needs a social regulation with international recognition, government first responsibility, social compensation, public sharing, priority of the weak and lasting effect(Tiankui Jing,2013). In this way, we will open up cooperation, create a loose development environment and build more cooperation platforms to lay the foundation for the governance of cyber security. It emphasizes the democratic and equal attributes of the Internet, maintains the social order of cyberspace, and recognizes that data security is not only a part of the global network strategic resources, but also an inevitable requirement for the development of the big data era, and one of the principles of global cyber security.

(3) Bearing in mind the global network “disaster”, avoiding historical reenactment, clarifying the real risks of the Internet, promoting the establishment of a internet global security governance mechanism, strengthening the four core layers of global network security, and finally forming a concentric structure of internet global security governance. The four core layers of global cyber security are as follows: To manage and standardize the key technologies of the Internet; To Incorporate key resources of the Internet into the regulatory system, such as website domain names and server systems; To Conduct monitoring and management of user codes of conduct, such as network spam, network fraud, etc.; For the industries derived from the development of the Internet, sound management regulations, such as intellectual property rights and personal reputation rights. Of course, with the development of the Internet, the governance of global network security has gradually formed, including key resources management, network information security, network development and construction, free flow of information, intellectual property protection, and economic and trade(Guo Feng,2012).

4. Conclusion

The main body of cyber behavior is composed of the Internet's audience - Internet users, Internet companies, Internet organizations, and Internet public power executors. As the main body of network behavior, in the process of global network security governance, it is mainly controlled by technical means, and the self-discipline of the network convention self-discipline, while still accepting the management of the state department and the supervision of the public. Although the Internet has spread to all corners of the world, it has many forms, such as public welfare organizations, groups, intergovernmental international organizations, non-governmental organizations, or regional associations, but so far, in addition to “the Internet Convention” and Outside “the Internet Treaties”, there is no globally recognized organization responsible for maintaining and managing the internet. In the global network environment, as the executors of the public power of the Internet, governments of all countries not only have the most network resources, but also have strong network control power. They have the responsibility to promote the improvement of the network environment, guarantee the orderly participation of the participants of network behaviors, and make contributions to the global network security sharing.

In addition, in the internet global security governance, the government as the main body of network security behavior, in addition to promoting the renewal of network technology, is more obliged to prosper the development of network culture, maintain network information security, participate in the construction of global network values, and develop global network security. The standards of behavior, as well as the spatial order of the global network, aim at the community of shared future in cyberspace security, advocate multi-agents, participate in a series of internal and external mechanisms, implement common maintenance and governance, ensure peaceful development, and share benefits.
Reference


[3] Huan Qiu. The world entered the era of "cyber cold war" and actively prepared for war with the United States and France.


[6] Pei Tong. Us hackers have hit bottom, with an estimated cyber army of more than 100,000.
