DOI 10.15302/J-SSCAE-2016.06.002

Research on the Issue of a Cyber Sovereignty Guarantee

Zou Peng[1], He Jun[1], Zou Hongxia[1], Liu Yunjie[2]

1. Academy of Equipment of PLA, Beijing 101416, China
2. China United Network Communications Limited, Beijing 100089, China

Abstract: As cyberspace carries more and more national, public, and private interests, the issue of a cyber sovereignty guarantee has attracted great attention around the world. From the perspective of China's cyber sovereignty situation, this paper analyzes the main problems related to China's cyber sovereignty guarantee, including the implications of the cyber rights of independence, equality, self-defense, and jurisdiction. Corresponding countermeasures and suggestions are also provided. The purpose of this paper is to promote the establishment of cyber sovereignty, strengthen China's discourse right on international cyberspace governance rules, and enhance China's ability to safeguard national cyberspace security interests.
Keywords: cyber sovereignty; cyber right of independence; cyber right of equality; cyber right of self-defense; cyber right of jurisdiction; cyber border defense

1 Introduction

China is a firm promoter and powerful maintainer of cyber sovereignty. In the roughly 20 years since the start of the Internet in 1994, cyber enterprises in China have undergone rapid development and made significant progress. However, during this period, unceasing threats and challenges in politics, security, and economy from some of the world's great cyber powers have driven China increasingly to elevate the strategic importance in an effective guarantee and defense of its cyber sovereignty, and thus gradually formed a strategical view of cyber sovereignty, featuring the advocates on the principle of respecting sovereign equality in cyberspace as its core value [1]. Although no strict and uniform definition of cyber sovereignty that includes the connotations and extensions of this concept have been internationally acknowledged, the basic principles of cyber sovereignty have been generally accepted by the international community, along with the increased benefits and conflicts that cyber sovereignty provides for the cyberspace of all nations. Under such circumstances, a guarantee of cyber sovereignty becomes the key to a nation's jurisdiction of its sovereignty. Cyber sovereignty is the extension and prolongation of national sovereignty into cyberspace. As an emerging economic and cyber nation, compared with the American-led western powers, China is at a disadvantage regarding its ability to impose cyber control, thus demonstrating the huge gap between its capacity to guarantee cyber sovereignty and its capacity to maintain national security interests, and the huge gap between China and other powerful nations in network confrontations as well. To address this issue, this paper examines the sovereignty issues that relate to cyberspace and discusses strategic measures for promoting cyber sovereignty. This study carries important practical significance toward enhancing China's right to discourse on rule making for international cyberspace governance and to maintain the benefits of China's cyberspace security. This paper raises relevant issues and countermeasures regarding cyber sovereignty from the perspective of a realistic demand for cyber independence, cyber equality, cyber self-defense, and cyber jurisdiction.

2 Guaranteeing the cyber right of independence

The main issue related to the cyber right of independence is whether the root domain name system (DNS) is manipulated by others. The current DNS adopts a centralized management

Received date: 16 October 2016; **revised date:** 22 October 2016
Corresponding author: Zou Peng, Academy of Equipment of PLA, Professor. Major research field is cyber security. E-mail: zpeng@nudt.edu.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 008–012
Cited item: Zou Peng et al. Research on the Issue of a Cyber Sovereignty Guarantee. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.002

structure. Thus, when a "netizen" (Internet user) requests a domain name resolution, the request is first submitted to the core root name server for resolution, if there is no cache; next, a stepwise recursive resolution is performed, guided by the root name. Therefore, if the root domain server fails, the whole DNS may become abnormal and may even collapse, resulting in netizens all over the world being unable to access the Internet.

There are 13 root domain name servers in the world, with 10 being located in the US, two in Europe, and one in Japan. Among these, the root server operated by VeriSign, Inc. is the main server, and the other 12 are slave servers that are controlled by the main server. In order to improve the efficiency and reliability of domain name resolution, many countries (including China) establish hundreds of mirroring severs of root servers. However, these are also controlled by the root server. In this way, the core hub and key basic resources of the global Internet have been controlled by the US. In unusual circumstances, the US can unilaterally cut or freeze the Internet in other countries, setting up the new strategic deterrence capacity of the US having a "switch" that controls the Internet.

In order to eliminate this risk from the root DNS to the cyber right of independence in China, a core solution involves presenting the technical solution of decentralization, building a self-governing root DNS, and forming an international root domain resolution alliance [2]. The core thought behind this solution—which is called the national independent root domain name alliance (NIRDNA) scheme—is to unite nations that are concerned about their cyber right of independence, in order to establish an alliance. The member states establish their root domain name servers through NIRDNA in order to replace the first resolution function of the root domain name server; thus, all requests for domain resolution do not point to the root domain name server, but rather to the local NIRDNA, and are then recursive to the root domain name server if no resolution information is available. NIRDNA is equal between nations, with each nation assigning its own top level domain (TLD) addresses (e.g., ".cn" for China, and ".ru" for Russia). The national NIRDNA can act as an agent for domain name resolution services for other allied members.

The NIRDNA scheme is characterized by openness, equality, autonomy, and compatibility. Any country can freely join or exit the NIRDNA system, the NIRDNA resolution service is open to global users, and people can freely choose a root name server as the first resolution. All nations involved in NIRDNA have equal status and do not control each other, and data of national root sever can be exchanged equally. The resolution service that is undertaken by the national NIRDNA is managed by a local domain name management institution. NIRDNA can coexist with the current domain name authorization management, and can operate without influencing the existing system. Some nations may select the NIRDNA resolution server, while others that prefer to keep to the status quo can choose to use the root domain name server. According to many international communications, the NIRDNA scheme has been recognized and praised by Russia, Cuba, and several Latin American countries.

3 Guaranteeing the cyber right of equality

The main issue related to the cyber right of equality is that the current DNS is formed by agreements between each country and the Internet Corporation for Assigned Names and Numbers (ICANN), where ICANN is Party A (the charterer), and each country is Party B (the lessee). ICANN is a non-profit organization that is registered in the US and that is under the jurisdiction of the US Department of Commerce. At present, if other countries want to change the IP of a TLD, they must place the change on record in the US Department of Commerce through ICANN. Therefore, China's national and regional TLD (.cn) still involves abiding by rules set by the US, which means no equality to China.

The internationalization of ICANN should be promoted in order to guarantee equal status for all countries on the Internet, transform the resources of the Internet back into the public property, and establish a common order that is under shared global governance. The United Nations will play a leading role in promoting the sharing and co-governance of cyberspace, all countries will participate equally in the governance of the Internet, and an international arbitration organization will be established for the resolution of major network conflicts. The internationalization of ICANN can realize the interconnectivity and interoperability among all countries in an equal way, thus changing the current inequality situations, in which a minority of countries owns the majority of network resources, and using this to make uneven distribution. On October 1, 2016, the US gave up its right to Internet resource management and handed this management over to multiple stakeholders; however, the unequal distribution of Internet resources has not been essentially changed.

4 Guaranteeing the cyber right of self-defense

At first glance, the main issue related to the cyber right of self-defense on an international level is the lack of a legal basis regarding international cyberspace attack and self-defense, as the party accountable for a cyber attack cannot be easily investigated. The *Charter of the United Nations* presents clear requirements for the right of self-defense of a sovereign state, including prerequisites, objectives, time, methods, and limitations. However, such requirements are designed for traditional wars that have a tangible, physical space (i.e., land, sea, air, or space) as their battleground; thus, these requirements are only suitable for hostile armed action with differentiable attack sources, and not for wars such as cyber warfare, which take place in a immaterial, virtual cyberspace. Since a cyber attack can effectively hide its source, the initiators can easily shift the blame onto others. If the current laws are simply and directly used in cyberspace, meaning

that a country may start a war based on doubt and without abundant proof, then the protective barrier that has been established by international law to prohibit the excessive use of force may collapse [3]. Therefore, international cooperation must be strengthened, under the framework of the United Nations, and the application of the international law of armed conflict to cyberspace must be researched in order to avoid a potential full military conflict caused by the excessive use of force.

China will organize and carry out research on the international law of armed conflict in cyberspace—on the one hand, by tracing and analyzing legislation trends in cyber warfare laws in the western states and, on the other hand, by carrying out a preliminary study on formulating relevant cyberspace legislations and rules in China. China will cooperate internationally to formulate laws for cyber warfare that will eventually benefits developing countries when time is right. For a developing country like China, the key goals right now are to build a technical reserve and construct a battlefield environment for armed conflicts in cyberspace as well as to propagate a stance that China opposes the cyber arms race and infringements on the interest of other countries through the Internet. Only in this way, can China gain moral supports from international communities.

Domestically speaking, there is no effective fortification of China's cyber boundary, and there are no effective defenses or countermeasures against a massive cyber attack. Guarding China's cyber territory is an important measure in defending cyber sovereignty. However, there is a lack in border establishments of cyberspace defense, such as boundaries and ports of territorial border. In addition to shortages in a cyber border defense system and in structural power, China also has a serious lack of capability to deal with and fight back against cyber attacks. The level of China's technological methods for cyber defense, attack tracing, and counter attacking is not high, and there is a lack of cyber defense weapons with an effective deterrent force. Institutionally speaking, there is no information sharing systems existing among the different departments, which restricts the development of China's cyber defense capability. Organizationally speaking, there is no armed defense forces protecting the cyberspace; that is, the military does not participate in ensuring the safety of China's cyberspace sovereignty. At present, the military's responsibilities regarding cyberspace are mainly to protect the military network; it has no specific responsibility for the civil network infrastructure. However, this current distribution of responsibilities does not completely agree with the historical mission of the military, which is to protect the sovereignty of the state, national security, and the territorial integrity in the current period. Therefore, it is important to define the military responsibilities in protecting China's cyberspace infrastructure and important information systems in the context of detriment to sovereignty, and strengthen the civil-military integration in building of a national cyberspace defense forces and constructing a national cyber border defense as well.

The term "cyber border defense" refers to a complete set of cyber defense and counterattack measures that are adopted to protect a nation's political, economic, military, and cultural benefits in cyberspace. In order to effectively improve China's support capability for its cyber border defense, and to elevate China's ability to deal with a large-scale cybersecurity emergency, we suggest starting a national cyber border defense construction project in order to form a cyber defense system that relies on the "national information gateway," with an integrated military and civilian cyber defense force as the main body, backed up by military cyber warfare troops. Suffice it to say, we suggest incorporating the nationally important cybersecurity infrastructure into a national system for cyber defense, and guiding this new cyber defense system with a holistic national defense philosophy [4]. The key point here is bringing all the important cybersecurity information systems of the cyberspace defense system into an operating mechanism which can realize a unifying management and linkage coordination. Therefore, it can shoulder more responsibilities which including guarding against cyberspace intrusion, filtering harmful information, authenticating cross-border electronic status, monitoring cross-border e-commerce, and so forth.

5 Guaranteeing the cyber right of jurisdiction

The main issues related to the cyber right of jurisdiction are: data jurisdiction problems that are caused by big data—that is, the data sovereignty problem; and online information supervision and management problems that are caused by the free mobility of information—that is, the problem of information sovereignty. Just as land and minerals are the core resources for territorial sovereignty jurisdiction, so are Internet-related data and information the core resources for cyber sovereignty jurisdiction.

Data sovereignty is a subset of cyber sovereignty that refers to the supreme power a nation holds over the generation, collection, transmission, storage, analysis, and use of all data—such as text, pictures, audiovisual material, codes, and programs—that are produced by individuals, enterprises, and other organizations located within the regime's jurisdiction territory. This right includes data ownership and data jurisdiction, where "data ownership" refers to the sovereign state having the exclusive possession of domestic data, while "data jurisdiction" refers to the sovereign state having the right to manage and use its data [5]. Data sovereignty means that even when data is transmitted to the cloud or to a remote server, they are still controlled by the main body of a state, rather than being manipulated by other countries or organizations. For international relations in the big data era, the issues concerning data sovereignty and its authority-responsibility mainly involve three parties: the enterprises, institutions, and individuals that are under the jurisdiction of the country where the data originated, the cloud service suppliers who own the actual management rights of the data, and the

sovereign state that possesses executive and legal jurisdiction. Since the technological levels of different nations in cyberspace are uneven, powerful nations are able to plunder data resources from weaker nations, a process that seriously violates the sovereignty of the weaker nations [6]. Particularly given the proven technology in the Internet of Things and cloud computing, big data can be acquired whenever and wherever, stored in trans-regional and cross-border locations, and spread freely in cyberspace. These conditions make data management extremely difficult. Competition for data rights among interest groups and sovereign states is becoming increasingly severe, bringing the issue of data sovereignty to the attention of countries around the world [7].

Information sovereignty refers to the supreme power a nation holds over information production, spreading, and transaction, and relevant organizations and systems within its political jurisdiction territory, including the protection, management, and control of information [8]. Issues related to information jurisdiction mainly concern the monitoring and management of online information. At the current time, the diversification of people's interests, the complexity of ideological struggle, the escalation of color revolutions, and the occasionally happening of information warfare through the Internet really do harm to state powers. A country that maintains its information sovereignty in cyberspace can build an environment of good and healthy information spreading and resource sharing. In contrast, a bad cyberspace information environment is one that is full of junk email, rumors of fraud, and Trojans and virus that harm information security, social security, and even national security.

The general requirements needed to execute cyber jurisdiction and effectively protect data sovereignty and information sovereignty are: at the legislation level, to actively promote relevant laws and regulations; at the system and mechanism level, to straighten out the functions among different departments and institutions, and to build a trusted cyber identification management system step by step. In addition, the importance should be attached to the general awareness of cybersecurity and the sovereignty guarantee within organizations and the public.

On a more detailed level, the cross-border transportation, storage, and use of data should be firstly specified. In order to limit cross-border data flow, the main international management trend is to establish a data center and store data within the borders of the state. Laws and regulations concerning a data protection have been introduced by nations and regions such as Russia, Japan, and the EU. Similar regulations for the cross-border transmission, storage, and use of data should be established in China as soon as possible. Second, through multilateral and bilateral negotiation and participating in international cooperation regarding cross-border data flow, common rules for cross-border data flow should be built to reduce the risks and cost caused by differences in regulations. In the name of network information freedom, China should resolutely oppose cyber powers that attempt to seize network big data belonging to other countries, perform unilateral control of data and information resources, or use their advantages in network information technology to damage the interests of other countries. Third, China should implement by force a trusted electronic identity management strategy in cyberspace, and strengthen public opinion monitoring and content management. Identity authentications are the basis for tracing cyber attacks and performing the cyber right of jurisdiction. In addition, unified network identity authentication will create a safe and credible network, reduce criminal acts such as Internet fraud and rumors, and avoid harm to the state sovereignty from anonymous attacks through the Internet. The exit and entry administration departments will handle temporary electronic ID cards for legal foreigners entering into China, and establish the network guard; the customs department will collect tariffs on online traded goods and perform other functions based on the electronic ID cards, in order to realize network customs; and the network security department will uniformly specify Internet behavior management, and build a defensive system for electronic information.

6 Conclusions

This paper researches issues related to a cyber sovereignty guarantee and to countermeasures around the four sovereignties—that is, the cyber right of independence, the cyber right of equality, the cyber right of self-defense, and the cyber right of jurisdiction. This perspective aims to address the most pressing and urgent issues related to a cyber sovereignty guarantee. The measures described here are very pertinent to the current situation, and need to be further implemented. Nevertheless, since the establishment of a cyber sovereignty system is a wide-ranging, multi-layered, and complex problem, research from the perspective of long-term system construction, integrated deployment, and strong planning, including the establishment and support of laws and regulations, the construction of systems and mechanisms, and the development of technical measures are also necessary.

References

[1] Shen Y. The US national cybersecurity strategy [M]. Beijing: Current Affairs Press, 2013. Chinese.

[2] Fang B X. Discussion about the resolution system based on autonomy root domain name of national league in view of "national cyber sovereignty" [J]. Information Security and Communications Privacy, 2014 (12): 35–38. Chinese

[3] Cui C Z. New trends of the main countries cybersecurity strategy in 2015 [J]. Journal of Information Security Research, 2015, 1 (1): 2–8. Chinese.

[4] Wu C G. The strategic thoughts on accelerating the Chinese cyber defense construction [J]. National Defense Science & Technology, 2012, 33(3):1–4. Chinese.

[5] Du Y Y. National data sovereignty in the big data era [J]. International Review, 2016 (3): 1–14. Chinese.

[6] Cai C H. Big data reformation and challenge in international relations [J]. World Economics and Politics, 2014 (5): 124–143. Chinese.

[7] Shen G L. Great state to unite people: data sovereignty and the national data strategy in a big data era [J]. Nanjing Journal of Social Sciences, 2014 (6): 113–119. Chinese.

[8] Niu B W. Legal definition of information sovereignty [J]. Journal of Beijing University of Posts and Telecommunications (Social Sciences Edition), 2014, 16 (4): 25–33. Chinese.