DOI 10.15302/J-SSCAE-2016.06.001

Research on Cyberspace Sovereignty

Fang Binxing[1], Zou Peng[2], Zhu Shibing[2]

1. Cyber Security Association of China, Beijing 100010, China
2. Academy of Equipment, Beijing 101416, China

Abstract: Cyberspace sovereignty, also known as cyber sovereignty, is the extension of national sovereignty to the platform of information and communication technology systems. This article defines cyberspace and cyber sovereignty, argues against several erroneous points of view that deny cyber sovereignty, and discusses the existence of cyber sovereignty.
Keywords: cyberspace; cyberspace sovereignty; stakeholder

1 On the meaning of "cyberspace"

Before researching cyberspace sovereignty, it is necessary to understand the concept of "cyberspace," the connotations of the word "cyber," and the range of meanings that are referred to by this word. It is generally recognized that the term "cyber," which refers to nodes and connection edges, is used to represent a multi-object and interconnected system. In real life, the information network can be abstractly summarized in the following way: "Connection links" (physical or virtual links) connect isolated "tip nodes" (producers and consumers of information) to achieve transmission among tip nodes through an "exchange of nodes" and to realize exchanges of loads among nodes. The term "load" refers to the data and information in a network, such as electromagnetic signals, optical signals, quantum signals, network data, and so on. Thus, a network contains four basic factors: tip nodes, switching nodes, connection edges, and loads.

The definition of "cyber" reflects the wide range of its meaning. Not only is the Internet accorded this feature, but also telecommunications networks, the Internet of Things, sensor networks, industrial control networks, radio and television networks, and other information networks that are composed of electromagnetic systems, which align with the "cyber" concept. Therefore, discussions of cyberspace should not be confined to the Internet. Many countries are formulating cyberspace strategies, which include an explicit definition of the term "cyberspace." In general, there are four kinds of definitions, as follows: ① The first kind of definition concerns only information and communication infrastructure. According to the US National Security Presidential Directive/NSPD-54/Homeland Security Presidential Directive/HSPD-23 [1], cyberspace means the interdependent network of information technology infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. ② The second kind concerns both information and communication infrastructure and the data it carries. According to Italy's 2013 National Strategic Framework for cyberspace security [2], "cyberspace is a man-made domain essentially composed of information communication and technology (ICT) nodes and network, hosting and processing an ever-increasing wealth of data strategically important for states, firms, and citizens alike, and for all political, social and economic decision makers." ③ The third kind includes humans, infrastructure, and data. According to Israel's Resolution No. 3611: Advancing National Cyberspace Capabilities [3], cyberspace is defined as "the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data." ④ The

Received date: 12 October 2016; **revised date:** 21 October 2016
Corresponding author: Fang Binxing, Chinese Academy of Engineering, Academician. Major research field is cyberspace security. E-mail: fangbx@bupt.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): 001–007
Cited item: Fang Binxing et al. Research on Cyberspace Sovereignty. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.001

fourth kind includes four factors: humans, infrastructure, data, and operations (i.e., activities). According to the Concept and Strategies of Cyberspace Security of the Russian Federation [4], cyberspace is "a sphere of activity within the information space, formed by a set of communication channels of the Internet and other telecommunications networks, the technological infrastructure to ensure their functioning, and any form of human activity on them (individual, organizational, state)."

1.1 An analysis of four factors of cyberspace

In essence, the concept of cyberspace comprises those of "cyber" and "space." "Cyber" includes both Infrastructure and data, where infrastructure includes tip nodes, connection edges, and switching nodes, and data refers to load. "Space" includes both characters and activity. Thus, cyberspace has four basic factors: facilities (carriers, namely infrastructure), data (objects, namely the load), virtual characters (subjects, namely the users), and operations (activity or behavior). Virtual characters, data, and facilities exert management in cyberspace, while management regulations often restrict activity. Therefore, in order to understand cyberspace activity, one must understand both the nature of its links and interactions, and its characteristic of being restricted by certain future regulations.

1.2 Defining "cyberspace"

Cyberspace can be defined simply as an artificial electromagnetic space, with terminals, computers, and network equipment as its carriers. People can calculate data and communicate through it to realize specific activities. In this space, people, machines, and things can be organically connected to interact with each other and to produce all kinds of life-changing information, including content, businesses, and controls.

To further analyze cyberspace, academic and technological definitions need to be put forward. Cyberspace can be academically defined as follows:

Cyberspace is an artificial activity space for humans that comprises virtual characters, also referred to as "cyber characters," and relies on ICT systems in order to operate generalized signals. A cyber character is the subject that produces and transmits information, thus reflecting human will. ICT systems include the Internet, all kinds of telecommunication networks and communication systems, all kinds of transmission systems and the radio and television networks, all kinds of computer systems, the photo-electromagnetic or digital information-processing facilities such as embedded processor and controller in the key industrial infrastructure. Generalized signals are electromagnetic signals that can be stored, processed, and transmitted, including optical signals, electronic signals, audio signals, magnetic signals, as well as the signals that can interact with electromagnetic signals such as quantum signals and biological signals, all of which are processed in the ICT systems to produce, store, operate, transmit and display information. Operation refers to the activities that reflects human will by means of generalized signals and ICT, including signal production, data saving, status modification, information transmission, and content exhibition, which are summarized as cyberspace activity.

In this definition, ICT systems, generalized signals, cyber characters, and operations jointly reflect the four factors of cyberspace, namely, facilities, data, virtual characters, and operations—that is, the comprehensiveness of facilities and data, the generalization, subjectivity, and initiative of virtual characters; and the intentionality of operations.

The United Nations does not often use the word "cyberspace" when discussing cyberspace issues; rather, it stresses the expression of ICT. Therefore, from the perspective of ICT activity, and being similar to cyberspace characters by other countries, this paper defines cyberspace with an administrative slant:

Cyberspace is an artificial space based on ICT infrastructures that support humans in conducting various activities related to ICT. ICT infrastructures include the Internet, all kinds of telecommunication networks and communication systems, all kinds of transmission systems and radio and television networks, all kinds of computer systems, and various embedded processors and controllers in key industrial facilities. ICT activities include the manual processes of creating, changing, transmitting, using, and exhibiting information.

2 On the meaning of "cyberspace sovereignty"

Sovereignty has the following "three sets of four" features: the four basic factors of territory, population, resources, and regime; the four fundamental rights of the right of independence, right of equality, right of self-defense, and right of jurisdiction; and the four basic principles of respect for sovereignty, mutual non-aggression, non-interference in each other's internal affairs, and sovereign equality. As an extension of national sovereignty, cyberspace sovereignty naturally inherits these features.

2.1 The "three sets of four" features of cyberspace sovereignty

2.1.1 The four basic factors of cyberspace sovereignty

The four basic factors of cyberspace sovereignty are cyber territory, virtual character, data, and activity regulation. Of these, cyber territory is equivalent to territory, virtual character is equivalent to population, data is equivalent to resources, and operation regulation is equivalent to regime. Specifically, cyber territory is a cyberspace carried by facilities consisting of an ICT system, virtual character is the main body of operating data in an ICT system, data is the electromagnetic signal form carried by the ICT system, and operation regulation comprises

the conditions that decide the achievement of real-time data operation.

2.1.2 The four fundamental rights of cyberspace sovereignty

The fundamental rights of cyberspace sovereignty are the right of cyberspace independence, the right of cyberspace equality, the right of cyberspace self-defense, and the right of cyberspace jurisdiction.

(1) The right of cyberspace independence: This is an important manifestation of sovereignty, and requires a country's Internet system, whether regarding resources or application technology, not to be constrained and intervened by others. However, the current global Internet depends on only 13 root name servers to resolve domain names, a situation that directly affects cyberspace independence of those countries that do not host one of the 13 root name servers. A feasible means to solve the problem involves adopting an architecture for a domain name system (DNS) root zone governed by an association of nations. This architecture will employ an idea similar to the equivalent diffusion of inter-domain routing in order to structure a "root name equivalent diffusion" method. It will not only allow the owners of top-level domains to report to an original root name server, but will also enable them to report their root zone information to other owners of national root name servers, free from the confinement of the original root name server [5].

(2) The right of cyberspace equality: This is an extension of the right of independence. It allows networks of countries to connect with each other on equal terms, in contrast to the current inequality of most countries' Internet statuses, due to unequal network resources. Regarding the international governance of the Internet, all countries, big or small, should have equal rights and should adopt the "one state, one vote" system.

(3) The right of cyberspace self-defense: This is also an extension of the right of independence. A nation has the right to protect its domestic cyberspace from external invasion, and it must build a military power that can protect its sovereign space. Firstly, a country should defend against external attacks by building a "network frontier defense" to protect its "sovereign network;" secondly, it should clarify its army's responsibility in protecting the national network infrastructure and important information systems, and give full play to the role of the regular army.

(4) The right of cyberspace jurisdiction: The right is to exert the sovereignty over the cyberspace within a nation's territory, which are actually performed by all the countries. Although some countries argue against the claim of cyber sovereignty, in reality, almost all countries impose strict management over their cyberspace, and prevent the interference from other countries.

2.1.3 Four fundamental principles of cyberspace sovereignty

Respect for cyberspace sovereignty involves respecting the right of cyberspace independence, rather than taking actions that impair the autonomous operation of a sovereign cyberspace. Mutual non-aggression involves not carrying out cyber attacks on other countries' cyberspace. Non-interference in each other's internal affairs involves not dictating the jurisdiction of other sovereign cyberspaces. Finally, cyberspace sovereign equality involves equal right of management over cyberspace among sovereign countries, rather than some countries losing this right while others control the global cyberspace due to a "stakeholder" pattern.

2.2 Defining "cyberspace sovereignty"

A general definition of cyberspace sovereignty is that it is a natural extension of national sovereignty over the cyberspaces carried by ICT systems located within that nation's territory, including activities performed by ICT systems (i.e., cyber characters and operations), ICT systems themselves (i.e.,facilities), and the associated data (i.e., cyber assets) that are under the jurisdiction of that sovereign state (which holds the right to intervene in manipulating the data).

From this perspective, ICT activities are virtual-character specific, and virtual characters are considered as population; ICT systems are facility specific, and facilities are platforms to carry cyberspace, which are considered as cyber territory; data carried by ICT systems are similar to virtual assets; and sovereign jurisdiction refers to the right to intervene with data and operations, which are considered as cyber regime.

Considering that cyberspace sovereignty contains the "three sets of four" features described above, a more precise definition of cyberspace sovereignty is as follows:

A country's cyberspace sovereignty is based on the ICT systems under its jurisdiction (cyberspace territory)，and the boundary of its function is defined by the collection of device ports that directly link the country to other countries (boundaries). Cyberspace sovereignty protects the various operations that virtual characters perform on the data (regime, user, and data). The facilities, data, and operations carried out within cyberspace is under the judicial and administrative jurisdiction of its hosting country (right of jurisdiction). In addition, the governing states of each country are equal in their management of international cyberspace (right of equality). Furthermore, the operation of ICT infrastructure within a country's territory cannot be interfered with by another country (right of independence). Finally, a country has the right to protect its cyberspace from infringement and to acquire military capabilities (right of self-defense). Cyberspace sovereignty should be mutually respected (respect for sovereignty); therefore, countries may not infringe on other countries' cyberspace (mutual non-aggression) or on their right to manage their cyberspace affairs (mutual non-interference in each other's internal affairs). The cyberspace sovereignty of each country has equal status in the governance of international cyberspace (sovereign equality).

2.3 Cyberspace sovereignty virtually exists in the affairs of countries around the world

Although many countries insist that stakeholders should dominate the Internet, and do not admit the existence of cyberspace sovereignty, almost all countries are in fact exerting their sovereignty in cyberspace. Therefore, conflicts in cyberspace can only be solved once and for all by governments. Proofs in recent years have shown that national sovereignty has, in fact, been exerted on the Internet. For example, the US combated online piracy by confiscating domain names [6]; the UK banned infringing websites [7]; Germany required the filtering of illegal information spread by the Internet [8]; the Indian government's ministry of telecommunications blocked websites [9]; Singapore opposed the spread of extremist content [10]; South Korea combated the spread of cyber rumors [11]; France cracked down on cyber racism [12]; and Israel combated online gambling [13].

3 On the conflict of sovereignty in cyberspace

Western countries, represented by the US, regard cyberspace governance as a technical level of governance. They stress freedom of connection and emphasize that the free circulation of information should not be hindered. Other countries, represented by China and Russia, consider content regulation to be one of the focuses of cyberspace governance, and advocate cyberspace sovereignty [14].

3.1 Views supporting the idea of cyberspace sovereignty

Not only do Chinese and Russian scholars actively support the idea of cyberspace sovereignty, but some experts in the US and in other western countries also hold the same view.

Articles published in *Air Force Law Review* [15] stated that cyberspace sovereignty exists for reasons including the following: ① Cyberspace requires a physical structure because, without one, users have no access. That physical structure, however, is terrestrially based and thus naturally falls under the purview of the state where those physical assets sit. ② Cyberspace needs laws to govern financial relationships and transactions. ③ The information that can be accessed by the users is constrained by the laws of the states where they reside. ④ States are increasingly required to assert their presence in cyberspace, as a matter of national security. ⑤ Many users see the Internet as a means of disseminating a specific message of hate or violence. Consequently, cyberspace needs a sovereign influence [15].

The US Senate Committee on Commerce, Science, and Transportation [16] has stated: "Cyberspace is not a global commons. It is a shared global infrastructure. There is rarely a moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state."

Eric Talbot Jensen, an expert from Brigham Young University in the US, has stated [17]: "As a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources."

In 2013, the *Tallinn Handbook of International Law Applicable to Cyber Warfare* [18] stated: "A State may exercise control over cyber infrastructure and activities within its sovereign territory," and "This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."

Scott L. Malcolmson of the Carnegie Corporation [19] has stated that "in some cases, Internet sovereignty can mean a state protecting its citizens' privacy against international corporate surveillance or infiltration by another state. In other cases, it can mean the state ensuring that it can invade the privacy of its citizens whenever and however it likes."

3.2 Views against the idea of cyberspace sovereignty

There are many reasons that lead to a repudiation of cyberspace sovereignty; however, such views are generally found to be one-sided after their implications have been analyzed.

Some argue that the Internet has no "cyberspace territory." For example, Microsoft's Azure cloud covers a vast region spread across the world. However, if a country's government ordered Azure to shut down its computing systems that are located within the territory of that country, the cyberspace these systems carried would naturally disappear. Thus, the cyberspace that is entrusted to a territory's ICT systems is subject to national sovereignty and cannot exist in a vacuum. In fact, the aim of the US cyberspace army is to protect cyberspace territory.

Some argue that the Internet has no borders, and thus has no territory or sovereignty. This argument was originally based on technical capabilities. However, if there is cyberspace territory, there must be a boundary. For example, North Korea's official website "By Our Nation Itself" (www.uriminzokkiri.com) is located in the Internet data center (IDC) room in Shenyang, China. However, this site is blocked by South Korea through filtering measures set at the Internet border.

Some argue that the Internet is a "global commons" over which no sovereignty exists. Compare the following situations: As it is a public act, international consultation and agreement are required in order to strike at piracy in the high seas of Somalia. However, when the US District Court for the Eastern District of Virginia ruled that the domain belonging to Maya Shanghai, cnnews.com, was an infringement of the Cable News Network (CNN) trademark, and that the Shanghai company must therefore stop using this domain, no international consultation is conducted and thus this action no longer followed the model of a

public act [20].

Some argue that cyberspace sovereignty is against the free flow of information. This argument is erroneous because of its misunderstanding of the source of the regulation involved. In the Schengen Area, people can move freely between countries; however, such movement is not proof of a lack of national sovereignty. Similarly, the free flow of information should comply with regulations that depend on the public policies of governments, rather than on those based on the existence of sovereignty. For example, the Counter-Terrorism Internet Referral Unit of the United Kingdom has secured the removal of 65 000 items from the Internet that encouraged or glorified acts of terrorism [21].

Some argue that the Internet is led by its stakeholders rather than by governments, and that there is naturally no sovereignty. From a technical point of view, it is reasonable to say that stakeholders play a central role in the Internet; however, from a public policy point of view, the Internet is clearly not led by civil users without administration identities. On December 12, 2003, the Geneva Declaration of Principles made by the United Nations and International Telecommunication Union (ITU) World Summit on the Information Society stated clearly that [22] "Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues." The Patriot Act of the United States authorized law-enforcement agencies to require Internet carriers to cooperate with intelligence demands. Thus, it has fully demonstrated the role and status of the government with regards to the Internet.

Some argue that there is virtual space sovereignty in cyberspace, and that this has nothing to do with the government. In 1997, Professor Tim Wu of the Columbia Law School [23] advocated virtual space sovereignty, stating: "States, their governments, and their citizens ought never to be taken for granted as players in cyberspace." In fact, if the Internet is an analogy of the market economy, it is notable that the government must still maintain order in the market economy. In 1998, with the rapid development of the Internet, the US announced its resumption of the management of Internet domain name ownership. Therefore, it is no longer objective to say that the Internet has nothing to with the government. Similarly, the government must be involved in deterring various cyber crimes, so it is rootless to assert that there is virtual space sovereignty.

3.3 Problems cannot be tackled by stakeholders alone

The Internet is significantly different from telecommunication networks, in that the Internet initially ran in the US, and other countries were invited to participate and given access. This means that other countries must follow the criterions set by the inventor. The US avoided dealing directly with other governments in the beginning, and therefore the stakeholders who contributed the most to the development of the Internet had speech rights. In essence, this stakeholder management model establishes a "law of the jungle": the stakeholders are the strong, and the weak only have the right to follow, not the right to make decisions or be heard. This model can also be interpreted as a certain strategy by which the US relinquished the management of the Internet Corporation for Assigned Names and Numbers (ICANN) and handed it to the stakeholders of the international community. To avoid being condemned as manipulating ICANN, the US government handed control to the international community as a strategy. Because US enterprises are "predators" at the "top of the food chain," this strategy maximizes the interests of the US.

However, it is not feasible to deal with problems by relying only on traditional stakeholders in the reality of the Internet.

(1) From the perspective of rational resource allocation, at present, ICANN is the distributor of the core Internet resources, which include IP address space allocation, domain name approval, and so forth. IP address space allocation, for example, is based on the application priority principle; its "first-come-first-serve" philosophy seems fair on the surface. In fact, however, it is the opposite of fair because some countries are limited by their development level and by their understanding of the importance of this resource. Only an organization made up of sovereign states would consider the inter-nation equality that is required to act fairly toward less-developed countries in issues such as these; such issues would not be considered by stakeholders.

(2) From the perspective of computer emergency response organizations, computer emergency response organizations are responsible for dealing with cyberspace security incidents. They are generally non-government entities, and belong to stakeholders. Because of their non-government identity, these organizations can only assist victim enterprises in a basic manner; it is difficult for them to trace the source of an attack and verify an attacker. Over time, transnational cyber crime will become a blind spot in laws and regulations. Therefore, in order to achieve effective cross-border cooperation, computer emergency response organizations require government authorization.

(3) From the perspective of cross-border e-commerce, the United Nations Commission on International Trade Law (UNCITRAL) is seeking consensus and viable options for laws and regulations on transnational identity management, which cannot be addressed simply by consulting stakeholders.

3.4 Starting points for China to advocate cyberspace sovereignty

At present, different countries' interests are in confluence or even conflicting with each other in cyberspace. What identity management model, for example, can be used to construct cross-border e-commerce systems? Allocating Internet resources is the same as allocating a carbon emission quota: Sovereignty

demands will appear. To this end, it is necessary to impose national sovereignty on cyberspace and to constitute an international co-governance system.

(1) Strengthening the international law status of states in the network era and promoting international co-governance of cyberspace: The popularity of the Internet has broken down the prestige of governments, as representatives of sovereign states, in their participation in international co-governance, and has made it possible for Internet stakeholders, by virtue of their technological superiority, to play a leading role in the development of the Internet. To maximize the Internet's positive impact on a global scale, and to ensure that all nations share the benefits from it equally, national sovereignty must be respected and all states must have the right to speak and make demands.

(2) Enhancing the state's right of speech with respect to the Internet in an international context: To play a responsible role in the international management of the Internet, China must increase its voice as a world power. By clarifying and introducing national sovereignty to cyberspace, sovereign states can participate in the Internet co-governance process.

(3) Maintaining political stability: Maintaining political stability is, in any case, an unshakable choice for all countries. However, the contradiction between the territoriality of a sovereign state and the transnationality of cyberspace has become a hindrance to controlling cross-border Internet behavior. Strengthening the concept of sovereignty in cyberspace will allow governments to defend their national sovereignty by controlling the input and output of information concerning cyberspace and the economy, as well as information relying on cyberspace defense lines.

(4) Protecting the basic data resources of the state: Traditionally, the input and output of geographical mapping and other important resources are strictly controlled by the state. However, great threats will occur if important digital data that is stored in cyberspace, including location information, medical information, and gene sample data, are poorly protected due to a lack of a clear definition of cyberspace sovereignty and of clear legislation.

(5) Constructing the foundation of cyberspace security: Discussions on the concept of cyberspace sovereignty have resulted in the naming of strategies to deal with cyberspace security events. They have contributed toward a common basis for people to understand the importance of cyberspace security and the notion that "if there is no cyberspace security, there will be no national security." Finally, they have laid the foundations for legislation, institution developing, mechanism establishing, and plan arranging.

(6) Regulating cyberspace according to the law: A clear definition of cyberspace sovereignty can provide legal support for a country's cyber activities. The government of China stresses that cyberspace be managed according to the law. It is suggested that the security of cyberspace and the healthy development of this country will be guaranteed by the development of appropriate laws regarding cyberspace management.

(7) Regulating the military presence: Military presence in cyberspace is based on the existence of cyberspace sovereignty. By strengthening the concept of cyberspace sovereignty, the responsibilities of the army in protecting key information infrastructures can be made clear, so that the army can actively defend the country's cyberspace border and play an important role in cyberspace confrontations between nations.

References

[1] The White House. National security presidential directive/NSPD-54 / homeland security presidential directive/HSPD-23 [EB/OL]. (2008-01-08) [2016-09-17]. http://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[2] Presidency of the Council of Ministers. National strategic framework for cyberspace security [EB/OL]. (2013-12-01) [2016-09-24]. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf.

[3] Israel R N. Resolution No. 3611 of the government: Advancing national cyberspace capabilities [EB/OL]. (2011-08-07) [2016-09-24]. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing%20National%20Cyberspace%20Capabilities.pdf.

[4] Russian Federation Council. Концепция стратегии кибербезопасности российской федерации [EB/OL]. (2014-01-10) [2016-09-24]. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.

[5] Fang B X. An analysis of the autonomous root domain name system based on the national cyberspace sovereignty [EB/OL]. (2014-11-27) [2016-10-03]. http://news.xinhuanet.com/politics/2014-11/27/c_127255092.htm. Chinese.

[6] U.S. Immigration and Customs Enforcement. Operation in our sites [EB/OL]. (2014-05-22) [2016-09-18]. https://www.ice.gov/factsheets/ipr-in-our-sites.

[7] Li M. The High Court of the United Kingdom ruled that Pirate Bay was in violation of copyright law [EB/OL]. (2012-02-20) [2016-10-06]. http://tech.sina.com.cn/i/2012-02-20/23526746542.shtml. Chinese.

[8] German regulatory body reported illegal material [EB/OL]. (2005-12-14) [2016-09-18]. https://www.lumendatabase.org/notices/9415#.

[9] Indian cyber silence: Journalists muted after race riots [EB/OL]. (2012-08-23) [2016-09-11]. https://www.rt.com/news/india-twitter-crackdown-riots-348/.

[10] Thread: Third racist blogger sentenced to 24 months supervised probation [EB/OL]. (2005-11-23)[2016-09-11]. http://forums.vr-zone.com/chit-chatting/44764-third-racist-blogger-sentenced-24-months-supervised-probation.html.

[11] Choi Jinsil commited suicide this morning, speculations led to the death of An Saiwan [EB/OL]. (2008-10-02) [2016-09-18]. http://ent.qq.com/a/20081002/000083.htm. Chinese.

[12] Comparis court rules Yahoo must screen French netizens from reaching nazi sites [EB/OL]. (2000-11-21) [2016-10-16]. http://

www.chinanews.com/2000-11-21/26/57081.html. Chinese.

[13] Hartman B. Police bust multi-billion online gambling rings [N/OL]. The Jerusalem Post, 2012-11-10 [2016-09-11]. http://www.jpost.com/National-News/Police-bust-multi-billion-online-gambling-ring.

[14] ITU. World conference on international telecommunications (WCIT-12) [EB/OL]. (2012-12-14) [2016-09-21]. http://www.itu.int/en/wcit-12/Pages/default.aspx.

[15] Patrick W F. Sovereignty in cyberspace: can it exit? [M/OL]. Colorado: U.S. Air Force Academy, Department of Law review, 2009 [2016-09-24]. http://www.thefreelibrary.com/Sovereignty+in+cyberspace%3a+can+it+exist%3f-a0212035708.

[16] U.S. Government Printing Office. Cybersecurity: next steps to protect our critical infrastructure–Hearing before the committee on commerce, science, and transportation United States Senate (One hundred eleventh congress, second session) [C/OL]. Washington DC: U.S. Government Printing Office. (2010-02-23) [2016-09-06]. https://fas.org/irp/congress/2010_hr/cybersec.pdf.

[17] Jensen E T. Cyber sovereignty: the way ahead [J/OL]. Texas International Law Journal, 2014, 50 (2): 275 [2016-09-21]. http://www.tilj.org/content/journal/50/14%20JENSEN%20PUB%20PROOF.pdf.

[18] The NATO Cooperative Cyber Defence Centre of Excellence. Tallinn manual on the international law applicable to cyber warfare [M/OL]. Cambridge: Cambridge University Press, 2013 [2016-09-08]. http://www.jku.at/intlaw/content/e275831/e275836/e276629/Tallinn_Manual_CW.pdf.

[19] Malcomson S L. The open, universal internet is over. But did it ever really exist? [EB/OL]. (2016-04-03) [2016-09-17]. https://www.theguardian.com/commentisfree/2016/apr/03/internet-web-politics-money-freedom-state. Chinese.

[20] Zhao X M. Legal integration is needed for transnational domain name disputes [EB/OL]. (2014-03-24) [2016-09-27]. http://ip.people.com.cn/n/2014/0324/c136655-24720867.html. Chinese.

[21] Home Office, Theresa May R H. Speech: Home Secretary Theresa May on counter-terrorism [EB/OL]. (2014-11-24) [2016-09-11]. https://www.gov.uk/government/speeches/home-secretary-theresa-may-on-counter-terrorism.

[22] The declaration of principles: building information society—A global challenge for the new millennium [EB/OL]. (2003-12-12) [2016-09-21]. https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf. Chinese.

[23] Wu T S. Cyberspace sovereignty? —The internet and the international system [J/OL]. Harvard Journal of Law & Technology, 1997, 10(3): 647 [2016-10-05]. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech647.pdf.