DOI 10.15302/J-SSCAE-2016.06.018

A Review of the Major Viewpoints on Cyber Sovereignty Around the World

Zhu Shibing[1], Zhang Xuebo[1], Wang Yu[1], Liu Yunjie[2]

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

Abstract: Cyberspace, while bringing us great convenience, poses some new problems and challenges. Cyber sovereignty, in particular, constitutes the basic principle for solving the conflicts of national interest aroused in the process of cyberspace development. In this paper, a review and an analysis of three typical viewpoints on cyber sovereignty around the world are provided; namely, advocating for cyber sovereignty, opposing it, or being indifferent to it. An overview of the attitudes of important international organizations and major countries toward cyber sovereignty is also provided. The purpose of this paper is to provide an objective description of the current status of cyber sovereignty.

Keywords: cyberspace; state sovereignty; cyber sovereignty; multiple stakeholders; information communication technology-related activities

1 Introduction

After half a century of development, networks, as represented by the Internet and mobile Internet, have brought us much convenience both in life and work. Along with this convenience come many new problems and challenges in such fields as national security, social stability, economic growth, and personal privacy. The United States and other developed countries have long been in leading positions in the development and governance of the Internet; they practice a governance mode of "multiple stakeholders." However, international conflicts of interest brought about by the development of the Internet cannot be solved conclusively by the United States and "multiple stakeholders" alone. Rather, the public policy issues related to cyberspace need the involvement of sovereign states. China and Russia are among the first to propose the principle of cyber sovereignty, the essence of which is a new international governance order in cyberspace respecting cyber sovereignty. In the research community, no global consensus has been reached on cyber sovereignty. International organizations, states, and scholars are divided on this matter: some advocate for it, some oppose it, and some are concerned about security but not sovereignty. It is therefore important to have a clear and in-depth understanding of this issue. In the next section, an overview of the viewpoints on cyber sovereignty will be given so that a foundation can be provided for further study.

2 Analysis of the typical viewpoints on cyber sovereignty

Throughout the world, arguments for cyber sovereignty are gaining momentum, with cyber sovereignty becoming progressively more of a focus of strategic gaming among major countries. Three different viewpoints on cyber sovereignty can be distinguished after review and analysis: those advocating for it, those opposing it, and those being indifferent to it.

2.1 Analysis of the viewpoints opposing cyber sovereignty

Those opposing cyber sovereignty argue that the Internet is a global public domain, and that cyberspace should not admit any sovereignty, nor is it possible to create sovereignty in it. They

Received date: 12 October 2016; **revised date:** 20 October 2016

Corresponding author: Zhu Shibing, Academy of Equipment of PLA, Professor. Major research field is information network and security. E-mail: 13910953181@139.com.

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 089–093

Cited item: Zhu Shibing et al. A Review of the Major Viewpoints on Cyber Sovereignty Around the World. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.018

also claim that the power of the Internet would be limited if sovereignty is exercised by states in cyberspace, and the Internet does not need any national government to manage it.

First, those holding the view that the Internet is a global public domain believe that the Internet is different from physical space in that the former is globally interconnected in itself, not subject to the jurisdiction or control of any state, and therefore is regarded as an international public domain just like the open seas or outer space. It does not make any sense to speak about sovereignty in cyberspace, a sphere without national borders. The most representative is the National Security Strategy published in 2009 by the United States. However, this viewpoint disregards the fact that there are cyberspace disputes, conflicts of national interest, situations where assistance from other people or states is necessary, or where cracking down on crimes jointly by states is required.

Second, "the new sovereignty theory" holds that governments have neither the right nor the power to manage cyberspace, stressing that cyberspace has an emerging global civil society with forms of organization, values, and rules such that cyber conflicts and illegal activities have special ways of settlement [1]. The proponents of this theory also claim that governments are not entitled to govern cyberspace, arguing that mapping statehood onto a domain that does not recognize physical boundaries is problematic [2]. The representative proponents include Professor David Post at Georgetown University and John Perry Barloo, a well-known Internet activist. The new sovereignty theory is a purely individualistic mindset, neglecting that the Internet is a carrier of the great interests of states and that the interests of individuals are aligned with those of the state. The new sovereignty theory presupposes that governments have no other motives than limiting the development of the Internet network, believing that governments should have neither power nor enforceable rules in cyberspace.

Third, the free flow of information will be restricted by the legal system of the state exercising sovereignty in cyberspace once sovereignty is established there, so cyber sovereignty is unacceptable. One of the most outspoken representatives of this view is Hillary Clinton, America's former Secretary of State, who delivered three speeches on "Internet freedom." She claimed that Internet freedom is the open form, and the free flow of information should be unrestricted by state sovereignty and has values worth advocating for with great efforts [3,4]. The "free flow of information" is reported to be a much-advocated principle in western countries, who have an intense desire for free information flow particularly today where the new world outlook of "human rights above sovereignty" is prevalent, so these nations are strongly against state restrictions on Internet information. However, for the purposes of cybersecurity, a variety of Internet supervision laws and regulations have been enforced and network monitoring systems of all kinds have been put in place in western countries. In the United States, the "EINSTEIN" operation is an example.

Finally, the proponents of the "multiple stakeholder" Internet governance mode believe the Internet is the network of builders and therefore should be controlled as before by "stakeholders," or the enterprises building, operating, managing, and using the Internet, rather than by governments. This theory has as in its basis the belief that "multiple stakeholders" have some jurisdiction in this virtual space, and they have their own arbitration rules. Some anonymous cyber activities, such as stepping attacks, can hardly steer clear of judicial issues. However, there is no likelihood of the existence of another independent jurisdiction in a sovereign state. Regulating and controlling network operators by means of laws is possible with the assistance of international cooperation, so it is evident that non-centralization tendency theory is hardly valid in practice.

2.2 Analysis of the viewpoints supporting cyber sovereignty

In the eyes of those supporting cyber sovereignty, the Internet is not a special domain, and cyberspace is a domain that admits sovereignty where states can and do have the power to exercise supervision, and where the international law of armed conflict applies.

First, it should be confirmed that cyberspace, rather than a special domain, is similar to the land, sea, sky, and space. James Lewis (Brown University) and Liaropoulos (Department of International and European Studies, University of Piraeus) argued in their papers that cyberspace is not a special domain [5,6]. Liaropoulos pointed out that cyberspace had been mistakenly described as a domain transcending physical space that is immune to state sovereignty and resistant to international regulation. Arguing that cyberspace is not a special domain and further demonstrating that cyberspace is a reflection of the current international system just like the other four domains (land, sea, sky, and space) needing state governance, albeit in its peculiar properties, has created a sound foundation for the existence of cyber sovereignty.

It then follows that cyberspace is a domain that has sovereignty, and cyberspace rules shall be created with respect for state sovereignty [7]. Furthermore, the rules applicable to cyberspace are essentially a reflection of the physical world, not separable completely from human and societal development processes. States can impose supervision on the Internet [8], can cope with cyberspace challenges [9], and have the right to develop their cyber capability according to their own conceptions and resources. As with what is being done by the government of Estonia, one state may choose to develop its cyber capability extensively so that this capability may be made available to citizens or, as with North Korea, the government can choose to shut off its Internet network border to resist external influences [10]. A state can protect its citizens' privacy from international corporate surveillance or infiltration by another state. Representatives of these proponents include Professor Tim Wu (Columbia Law

School), Topi Tuukkanen (Finnish National Defence University), Patrick Schmitz (Vanderbilt University in the US), Eric Talbot Jensen (Brigham Young University Law School in the US), and Researcher Scott L. Malcomson (Carnegie Corporation). It is pointed out in the first chapter of the *Tallinn Manual* that sovereignty means that the state has the authority to control the network infrastructures within its territory and cyberspace activities within its territory [11].

Cyber sovereignty provides a basis upon which international cyber conflicts may be solved, as is recognized by Eric Talbot Jensen. He pointed out that the Internet breaks the traditional notion of boundary, and most doctrines of the Internet are still applicable to international armed conflicts, though some evolved versions of stipulations applicable to Internet era shall be added [12].

In addition, state governance in cyberspace exists in many countries. For instance, many countries have passed acts on cyberspace administration, such as the Adolescent Protection Act, the Anti-Junk Mail Act, and the Information or Data Protection Act. Some countries, the United States being one of them, have created cyberwar troops whose battlefield is cyberspace, and this is an obvious indication of state sovereignty enforced on cyberspace and the recognition of cyber sovereignty.

2.3 Analysis of the viewpoints that cyber sovereignty is not important

Aside from viewpoints expressly supporting or opposing cyber sovereignty, there is another viewpoint that cyber sovereignty is not a matter of importance. This viewpoint is reflected by some states which, for the purposes of safeguarding their own interests, place more stress on security in cyberspace and are concerned with better efficiency in protecting their network infrastructures against attacks and in protecting privacy and intellectual property rights. For example, Russia launched cyber attacks against Estonia in 2007, greatly downgrading the Estonian government's communication capability. Thus, the Estonian government espousing views on country borders is not sensible when dealing with cyber threats, and instead international cooperation is the key to restraining cyber attacks.

However, some developing countries have not yet touched on the issue of cyber sovereignty because of a lack of advanced Internet technology and network infrastructure.

3 Attitudes of international organizations and major states towards cyber sovereignty

3.1 International organizations led by the United Nations

Given the situation as it is, the United Nations (UN) admits that there is true cyber sovereignty, although it does not use the term "cyber sovereignty." Given the trend toward safeguarding the interests of most countries, the UN is to advance the formulation of a convention on cyber sovereignty and its protection throughout the world.

Document A/68/98 was published by the UN on June 24, 2013, adopting the resolution proposed by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [13]. The notion of cyber sovereignty is recognized in Article 20: "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." This is reiterated in Article 27 of Document A/70/174, a report published in July 2015 by a new group consisting of governmental experts from 20 countries [14].

The Geneva Declaration of Principles, adopted in the first phase of the conference of the World Summit on the Information Society on December 12, 2003 in Geneva, points out in Article 49 a) that "Policy authority for Internet-related public policy issues is the sovereign right of States." The Tunis Agenda for the Information Society adopted in the second phase of its conference in 2005 in Tunis includes a similar statement to that in Article 35 of the "Principles": "We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations."

The International Telecommunication Union (ITU) reviewed and adopted International Telecommunication Regulations in December 2012 in Dubai with the intent to place the Internet under the jurisdiction of the ITU, an organization sponsored by sovereign states, and allow states to manage the operation of the Internet and to regulate the Internet. The rules suggest that the ITU has the allocation rights for a small portion of all Internet addresses. This proposal, though strongly opposed by the United States and Europe, was adopted with the support of most votes, as the ITU did not follow the tradition of unanimous support to adopt the proposal.

3.2 The United States

Given the current situation, the United States practices a double-standard strategy in cyber sovereignty. On the one hand, for the sake of global dominance it asserts "global public domain" and "Internet freedom," and on the other hand it resorts to strategies and measures like ultra-strong control, all-around deterrence, aggressive interference, and a broad alliance to safeguard its own cyber sovereignty and security. Given the trend, the United States has no alternative but to acknowledge cyber sovereignty bit by bit, however it may seek a strategy of "taking what is agreeable and rejecting what is disagreeable" to create an international cyber sovereignty system in its own favor.

Clear from the "Internet freedom" premise is that the United States is attempting not to be restrained by the traditional sovereignty notion, and its focus is on expanding the scope of USstyle network governance and on augmenting its state interests, i.e. an "Enclosure Movement" in cyberspace. The US government criticizes other states for restricting Internet freedom, which amounts to selling its "freedom" values to other countries. Backed with its exceptional advantages in information technology, its control of the Internet root servers, and its information industry and market strengths, The United States is practicing political publicity, value tutoring, and thought transmission by means of the Internet so as to be ultimately in control of cyberspace and reinforce its global dominating position in the cyber domain.

3.3 EU member states

Judging from the situation, the European states generally share the basic viewpoint of the United States on cyber sovereignty while being particularly concerned with their own cybersecurity and sovereignty in cyberspace. They are likely to gradually acknowledge and support cyber sovereignty, but their action is under the control of others and hence they are unable to do what they like.

The European Union published the Cybersecurity Strategy of the European Union: Commitment to the European Countries Strengthening Security in Cyberspace, and the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace in 2012–2013, attesting to its positive attitudes towards safeguarding security in cyberspace. On the other hand, the European Union once suggested having the Internet Corporation for Assigned Names and Numbers (ICANN) headquarters in Geneva, which was vetoed by the United States. The European Union then proposed at the UN World Summit on the Information Society held at Geneva in 2003 that it should create a "cooperative mode" between governments to manage the Internet, which was quelled by the United States. It should be noted that the European Union is not free in its activities because it is restrained by the United States.

The UK, France, and Germany are forerunners of informatization and networking. The Internet has not only an extensive basis of e-governance and e-commerce, but also has permeated into critical infrastructures like energy, transportation, telecommunications, electricity, and taxation. These states, though not having any well-defined cyber sovereignty assertions, have one after another formulated their own state cyber security strategies, seeking to reinforce the protection of critical network infrastructures through various technologies and administrative measures.

3.4 Russia and developing countries

The present situation suggests that Russia, Brazil, and the Shanghai Cooperation Organization (SCO) are among the most proactive players supporting cyber sovereignty. The trend is that the emerging giants (blocs) have a strong desire to get involved in the game of strategic cyberspace interests and, because of their adequate economic and technological prowess, may become active proponents of cyber sovereignty.

Russia adopts an alliance strategy to address the issue of cyber sovereignty, asserting on several occasions that states shall enforce Internet regulations. To this end, Russian allies and other states by way of international cooperation to promote cyber sovereignty are forceful players in safeguarding cyber sovereignty. Russian President Vladimir Putin commented in 2014 when interviewed by Latin American and Russian media that state cyber espionage activities against one another are a violation of state sovereignty. Repeatedly, Russia has advocated state monitoring and regulation of the Internet. The Russian representatives presented cyber sovereignty and other proposals at the Dubai ITU conference in December 2012.

Brazil is supportive of the idea of cyber sovereignty, and denounces e-spying and other espionage activities in cyberspace, regarding it as a violation of state sovereignty. Brazil works with China to forge a strategic partnership on cyber sovereignty.

Apart from Russia and Brazil, other developing countries showing active support of cyber sovereignty include Belarus, Pakistan, Egypt, and Saudi Arabia.

4 Conclusions

In summary, western countries, particularly the United States, are strongly against cyber sovereignty, attempting to guard their interests and practice cyberspace hegemony. Many developing countries, on the other hand, are anxious to expand their interests and safeguard their cyber security, and are supportive of cyber sovereignty. After several confrontations in the UN and the ITU, those asserting cyber sovereignty are gaining ground by winning the support of an increasing number of states. Cyber sovereignty has so far become the principle to solve international conflicts of interest in cyberspace; asserting that the importance of cyber sovereignty is in the interest of most developing countries and is in line with the trend of the epoch as well.

References

[1] Gao H J, Tsinghua journal of rule of law (fourth edition) [M]. Beijing: Tsinghua University Press, 2004. Chinese.

[2] Post D G. In search of Jefferson's moose: Notes on the state of cyberspace [M]. New York: Oxford University Press, 2009.

[3] Clinton H R. Speech on internet freedom [EB/OL]. (2010-01-23) [2016-09-12]. http://www.checkinnews.cn/EditText_view.action?-textId=67582. Chinese.

[4] Clinton H R. Speech on internet freedom II [EB/OL]. (2011-01-23 [2016-09-12]. http://blog.renren.com/share/307262991/5137535771. Chinese.

[5] Lewis J A. Sovereignty and the role of government in cyberspace [J]. Brown Journal of World Affairs, 2010, 16 (2): 55–65.

[6] Liaropoulos A. Exercising state sovereignty in cyberspace: An

internal cyber-order under construction? [C]// Hart D, editor. Proceedings of the 8th international conference on information warfare and security ICIW 2013. Denver, Colorado, USA: Academic Publishing and Conferences International Limited, 2013: 136–145.

[7] Lindsay J R, Cheung T M, Reveron D S. China and cybersecurity: Espionage, strategy, and politics in the digital domain [M]. London: Oxford University Press, 2015.

[8] Wu T S. Cyberspace sovereignty?—The internet and the international system [J]. Harvard Journal of Law & Technology, 1997, 10 (3): 648–655.

[9] Tuukkanen T. Sovereignty in the cyber domain [M]// Rantapelkonen J, Salminen M, editors. The Fog of Cyber Defence. Helsinki: National Defense University, Department of Leadership and Military Pedagogy, 2013: 37–45.

[10] Jensen E T. Cyber sovereignty: The way ahead [J].Texas International Law Journal, 2014, 50 (2): 275–304. http://www.tilj.org/content/journal/50/14%20JENSEN%20PUB%20PROOF.pdf.

[11] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Tallinn manual on the international law applicable to cyber warfare [M]. Zhu L X, Zhu Y X, Chen W, et al, translators. Beijing: National Defense Industry Press, 2016. Chinese.

[12] Jensen E T. Sovereignty and neutrality in cyber conflict [J].Social Science Electronic Publishing, 2011, 35: 815–841.

[13] United Nations. Sixty-eighth session, item 94 of the provisional agenda: Group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/68/98) [R/OL]. (2013-06-24) [2016-09-10]. http://www.mofa.go.jp/files/000016407.pdf.

[14] United Nations. Seventieth session, item 93 of the provisional agenda: Group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174) [R/OL]. (2015-07-22) [2016-09-10]. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&lang=C.