Universe Scientific Publishing

DOI: 10.18686/ahe.v6i12.5032

On the Dilemma of International Governance in Cyberspace and China's Strategy

Zexi Wang

Law School，Anhui University of Finance and Economics，Bengbu233030，China

Abstract: With the growing prominence of cybersecurity threats, it brings challenges for countries to participate in international governance in cyberspace. Due to the different ideologies and network technology strengths of countries, this has led to controversial identification of cyberspace sovereignty, inadequate international rule of law in cyberspace, and imbalance of governance power in cyberspace, which has led to a governance dilemma. As an important participant in the international governance of cyberspace, China should respect the sovereignty of cyberspace, promote the international rule of law process, and advocate global collaborative governance.

Keywords: Cyberspace；International Governance；Cyberspace sovereignty；China's plan

Introduction

There has been a gradual increase in cybersecurity threat incidents in various countries, and the scope of impact has shifted from the domestic community to the international community. The journey of cyberspace governance is divided into three stages: from individual regulation to internal governance of sovereign states, and then to cooperative governance of the international community. However, the differences in cultural backgrounds and interests of countries have exacerbated the dilemma of international governance in cyberspace. China has also faced serious cybersecurity issues in recent years. In response, China should more actively participate in the international governance of cyberspace and improve domestic cyber governance approaches.

1. International governance dynamics in cyberspace

The international governance pattern of cyberspace currently includes three aspects. The first is the formation of a "dual-track" multilateral cooperation between UNGGE and UNOEWG to ensure the effective participation of sovereign states and multi-stakeholders in the international governance of cyberspace.In terms of content, UNGGE focuses on international regulation of state action in cyberspace and means of resolving international disputes, while UNOEWG builds on UNGGE's existing reports and makes more specific recommendations on norms, principles and threats to information security in cyberspace.[1]The second is that regional international organizations have formed some representative international treaties that provide multiple outlets for countries to participate in governance. Typical international organizations are ASEAN , Shanghai Cooperation Organization and EU. In November 2001, EU introduced the Convention on Cybercrime. In 2011, SCO member states submitted a draft International Code of Conduct on Information Security to the United Nations.The third is the active promotion of cyberspace governance by non-state actors, such as multinational corporations and international law scholars, to promote the development of cyberspace norms.Microsoft signed the Cybersecurity Technology Pact with Facebook, Dell and other technology companies.The NATO Cyber Cooperative Defense Center of Excellence Invited International Group of Experts to prepare Tallinn Manual on the International Law Application to Cyber Warfare and Tallinn Manual 2. 0 on the International Law Applicable to Cyber Operations.The two manuals systematically cover cyberspace sovereignty, jurisdiction and state responsibility. In essence, it is an elaboration of existing real international law at the level of cyberspace, which has important theoretical and practical values.[2]

2. The International Governance Dilemma in Cyberspace

2.1 The determination of sovereignty in cyberspace is controversial

Many scholars consider cyberspace as the "fifth space". Cyberspace has become a new type of space after the sea, land, airspace and outer space.[]Therefore, the applicability of sovereignty in cyberspace is controversial and mainly divided into two positions.The first one is the developed countries centered on the United States, which promotes liberalism and believes that there is no sovereignty in cyberspace, holding the "global commons theory". The second is the emerging Internet countries led by China and Russia, which are relatively more conservative and hold the "cyber sovereignty theory".The state has the right to regulate compliance and control cyber security in cyberspace. The analysis behind the two positions is actually the different ideologies of different countries.

2.2 Insufficient international legal regulation in cyberspace

International law includes international hard law and international soft law, with "hard law" norms usually embodying obligatory and prohibitive rules, and "soft law" norms characterized by "non-treaty binding".[]In terms of international hard law regulation, sovereign states generally lack the will to develop new international norms. Therefore, it mainly relies on the appropriate modifications of traditional international law that continue to function in the existing cyberspace governance.However, traditional international law has a lagging nature and cannot cope with the emerging issues of the network. Emerging cyber developing countries are also keen to

develop new international norms to safeguard their rights and interests.In terms of international soft law regulations, the main ones are UN General Assembly resolutions and documents.However, UNGGE and UNOEWG do not change the rights and obligations of States under existing international law, nor do they make additional provisions for other aspects of cyber attacks.

2.3 Imbalance of power in cyberspace governance

The process of international governance of cyberspace was initially dominated by the United States, followed by a stalemate between cyber developed and developing countries.Networked developed countries hold the major voice and governance with their inherent advantages in the cyber domain and advanced Internet technologies.The United States and other Western countries believe that globally connected cyberspace can be an important channel for traditional Western ideology and values.[]In contrast, network developing countries are disadvantaged in terms of technology and strength, resulting in the inability to effectively structure the international network system.Some Western countries have a monopoly on online discourse, and developing countries are eager for the right to speak.

3. Ways to Respond to International Governance in Cyberspace

3.1 Upholding the primacy of sovereignty in cyberspace

To solve the problem of international governance in cyberspace, the principle of cyber sovereignty should be adhered to first and foremost.Cyber sovereignty is a natural extension of national sovereignty in cyberspace.[]For cyber developing countries, only when they are recognized as sovereign in cyberspace in the process of participation in international governance can they have a legitimate reason to participate in international governance cooperation such as multilateral and bilateral.Therefore, China should first observe the principle of cyber sovereignty and regulate and control the activities in cyberspace on its territory.Second, to then engage in international cooperation as a cyber-sovereign state to counter attacks that violate cyber sovereignty.Finally, advocate cyber sovereign equality to other countries and enhance the discourse of cyberspace governance.

3.2 Promoting the international rule of law process in cyberspace

At the international level, promote the improvement of international hard law and pay attention to the role of international soft law.China should strive to make international hard law establish the principle of sovereignty in cyberspace, promote the revision of the original international hard law, and conclude relevant international treaties.It also provides a platform for the formation of soft law and organizes events such as the World Internet Conference and Summit.At the domestic level, the Cyberspace Strategy can be promulgated at an appropriate time to systematically announce the policy intention and mode of action for China's cyberspace governance, and to continuously improve the domestic Internet management system.In the global system of governance in cyberspace, there is a continuous dynamic interaction between international and domestic rule of law that affects each other.[]

3.3 Advocating global construction of a community of destiny in cyberspace

The Internet is global in nature, and no country can build an effective cyber defense mechanism by relying on its own strength alone.[]China believes that if an organism for cyberspace governance can be formed under the UN framework, it will be able to connect developed and developing countries to jointly address cyber risks.Based on this, first of all, China should actively collaborate with the international community to govern cyberspace and take the initiative to explain to other countries the meaning of the community of destiny in cyberspace.Secondly, it is necessary not only to actively carry out regional cooperation and exchange with sovereign countries, but also to promote the participation of network experts, network technology enterprises and others in governance.Finally, China should promote the construction of cooperation mechanisms. It should both learn Internet technology from developed countries and lend a helping hand to countries that are lagging behind in technology.

4. Conclusion

international governance of cyberspace is an important issue for the international community and concerns sovereign national security, economic development and people's lives.At present, in the process of international governance, there are large differences among countries in the concept of governance and the way of governance.As an emerging cyber power, China should actively promote the international governance process and strive to build an international cyberspace of shared governance, equality and win-win situation.

References:

[1]Li Hongyuan. 2008(08).On Network Sovereignty and the New Concept of National Security [J]. Administration and Law.

[2]Cui Wenbo.2013(03).The Impact of "Tallinn Manual" on my country's Cyber Security Interests [J]. Journal of Jiangnan Institute of Sociology.