Comment and Analysis on the Major National Strategies of Cyberspace

Tongyun Han[1, a], Yuhang Zhang[1, b]

[1]School of Public Administration, Nanjing Normal University, Jiangsu, China.

[a]hantongyun9449@163.com, [b]13260807877@163.com

Abstract

Since the birth of cyberspace, in order to seize the growth opportunities of the network information technology, expand the national network territory, and safeguard the national network security, countries have formulated the national strategies of cyberspace. Recently, with the breakthrough development and wide application of information technology in key areas such as "Big Data, AI, IOT and Cloud Computing", the development capacity for network has become an important support for national economic, political and cultural development. Countries are racing to speed up the pace of improving national cyberspace strategy, promulgating laws and regulations, strengthening the training of technical personnel, setting up cyberwarfare departments to deal with cyberattacks, and conducting joint cyberspace military exercises. The increasingly fierce competition in national cyberspace strategies has become an important factor affecting the peaceful development of international cyberspace. National cyberspace strategy, as a specific action plan for a country to guide the network construction and development of national cyberspace, and participate in global governance of cyberspace, is inevitably constrained by the actual national comprehensive strength in its formulation and implementation. As a real-time mapping of the real world, the differentiation of network developed countries, network developing countries and network underdeveloped countries has gradually emerged, and their national strategies are characterized by offensiveness, defensiveness and dependence, which have a profound impact on the process and development of global cyberspace governance.

Keywords

Cyberspace strategy; Cybersecurity; Offensive; Defensive; Dependence.

1. INTRODUCTION

In the development process of cyberspace, there are layers of national strength in the aspects of network security maintenance, data resource storage, key infrastructure construction level and international network discourse power in various countries and regions: the United States as the representative of the earliest network developed countries relying on the advantages of traditional economy, military and science and technology; China and Russia as the representative of although However, the network construction started late, but it depends on the number of Internet users, economic growth or national will to carry out the network construction, and advocates the establishment of a fair and open global network governance system in the network developing countries; the network coverage rate is low, the network operation quality is unstable, and the network development autonomy is weak in the network underdeveloped countries represented by the vast African continent countries. As the "fifth space" for human survival and development, cyberspace is rich in resources and development opportunities, and has become a new field of game among countries. In order to maintain and develop national interests, countries have formulated their own cyberspace strategies. In response to the dilemma of global cyberspace governance, although the network strategies of these countries have shown their strengths, they have achieved little in practice, and some of them have even further intensified the contradictions.

2. OFFENSIVE CYBERSPACE STRATEGY: INTENSIFYING COMPETITION FOR NETWORK RESOURCES

Offensive cyberspace strategy refers to a national strategy that relies on strong information technology strength and international influence to publicize national values in cyberspace, and to interfere with the construction of cyberspace in other countries on the basis of maintaining national superiority and security.

2.1 Typical Representative of Offensive Cyberspace Strategy: the USA

The U.S. government began to pay attention to the threat from cyberspace and the construction of key network infrastructure in the 1990s. At the same time, the U.S. government began to formulate a national network security strategy. The Clinton administration focuses on maintaining the privacy and security of network information, attaches importance to the protection of key infrastructure in cyberspace and the establishment of information security technology framework, so as to establish a "comprehensive defense" network security strategy. In 2000, the national security strategy in the global era was signed and passed, which marks that the U.S. government formally incorporated the cyber security strategy into the framework of the national security strategy, and the Clinton Administration's "comprehensive defense" strategy moved to the "deepening defense" stage. The "9.11" incident accelerated the decision of the U.S. government on the implementation and further refinement of the cyber security strategy. The Bush Administration formulated the cyber counter-terrorism strategy of "combination of attack and defense" in response to the "9.11" incident, redefined the scope of key infrastructure and signed the national infrastructure protection plan for maintenance. During the Obama administration, the strategy of "cyber deterrence" was formulated on the basis of the theory of "cyber power", and the national cyber security Promotion Committee was established to strengthen the coordinated management of cyber security affairs, while improving the construction of cyberspace security system to enhance the ability of network defense, awareness and traceability of cyberspace situation, cyberspace action and cyberspace law enforcement. In June 2009, the U.S. Department of defense established the cyber command, which is responsible for the cyber war. It shows the determination of the U.S. government to maintain the security and interests of the national cyberspace with military strength. At the same time, it exposes the Obama administration's ambition to seize cyber resources relying on military strength.

At the beginning of Trump's term in office, he made it clear that in order for the United States to obtain real security, the maintenance of network security must be put in the first place. On December 18, 2017, trump issued the first national security strategy report during his first term. He emphasized that the United States will curb, prevent and crack down on hackers who use cyberspace capabilities to invade the United States. At the same time, the trump administration proposed to let cyberspace reflect the values of the United States, safeguard freedom, safeguard the national security of the United States, and promote the development of the American economy. This highlights the trump administration's more pragmatic and competitive offensive network strategy. On September 20, 2018, trump Administration issued the first comprehensive document on the U.S. cyber strategy, the National Cyber strategy, which clearly stated that the U.S. government will try its best to make the U.S. have the best cyber security in the world, and take "offensive" actions with rich cyber weapons to deal with cyber threats and attacks, so as to protect the security of U.S. citizens in cyberspace. On the basis of protecting the network security and technological advantages of the United States, the government has integrated the network into all elements of national power, "maintaining peace by strength", enhanced the ability of the federal government to control network risks, so as to ensure that the United States has become a world leader in all fields including cyberspace. It can be seen that the national network strategy is the trump administration's priority governing program in the network world.

2.2 Evaluate Offensive Cyberspace Strategy

Although the cyberspace strategies formulated by successive US presidents have their own priorities, their cores for maintaining US cybersecurity and development interests are consistent. Relying on the United States' accumulated resources and technological advantages in cyberspace, it has gradually shifted from defensive counterattacks to active attacks, and at the same time, its offensiveness has increased significantly.

The offensive cyberspace strategy is based on the strong national cyber power and development capabilities. It includes a comprehensive national cybersecurity strategy of technology, talents, institutions and legal systems. It aims to vie for leadership in international cyberspace, takes the development dividends brought by data and information resources as its endogenous drive, takes the maintenance of national cybersecurity as its external drive, and takes cyber hegemonism and realism as its core. The offensive cyberspace strategy has helped the developed nations in the cyberspace led by the United States to establish their national advantage in cyberspace, cultivated a group of top talents and companies in cyber information technology, monopolized the management of root servers, and created a comprehensive, efficient, and independent Cyber Combat Force. All these have effectively safeguarded the national cyber security and development interests.

With the increasingly fierce game of dominant power in cyberspace, the implementation of offensive cyberspace strategy further intensifies the competition for cyberspace territory and resources among major countries, which is becoming more and more explosive. The western network powers led by the United States have introduced the traditional international political games into the international cyberspace without any taboo. They regard China, Russia and other countries as their biggest enemies in cyberspace. They take cyberspace governance as a means of game between countries. They try to launch the network driven economic and diplomatic war and spare no effort to promote the militarization and militarization of cyberspace. All these hinder the establishment of cooperation and trust among cyberspace countries, and at the same time, it is not conducive to the effective operation of the international governance mechanism of cyberspace, and it also squeezes the cyberspace living space of developing and underdeveloped countries, leading to the deepening of the "digital divide" and the increasing competition for cyber armaments. The hegemonic logic behind the offensive cyberspace strategy is gradually understood by all countries after the "prism gate" incident, which has inspired the will of all countries to speed up the reduction of the gap with the United States and the determination to safeguard the national network sovereignty. The white-hot trend of global cyberspace governance is gradually showing. This has further impacted the position of the United States as the global leader of cyberspace technology, making trump government's sense of security in cyberspace continue to decrease, and its aggressiveness further sharpened.

In short, the offensive cyberspace strategy, by "adding chaos" to the international cyberspace, makes all countries jointly bear the cost of the United States to defend its dominant position in cyberspace, which is a kind of national policy with the priority of the United States.

3. DEFENSIVE CYBERSPACE STRATEGY: IT IS DIFFICULT TO OBTAIN THE DISCOURSE POWER OF INTERNATIONAL CYBERSPACE GOVERNANCE

The defensive cyberspace strategy is mainly adopted by developing countries. Objectively, although the developing countries have certain network strength and development foundation, the gap between them is still obvious; subjectively, developing countries have realized that there is no national security without network security, and actively plan to build a network defense department to safeguard national network information security and national network development interests, trying to improve their network hardware In order to deal with the invasion from the developed countries and the cyber Mafia forces, we need to improve the level and governance ability.

3.1 Typical Representative of Defensive Cyberspace Strategy: China

In 2013, the outbreak of "prism gate" event, coupled with the white-hot game between China and the United States in cyberspace, prompted the awakening of China's cyberspace strategy. The new leadership began to focus on the governance reform of cyberspace and capture the huge development opportunities brought by cyberspace. In 2014, a leading group of central network security and informatization was set up. Chairman Xi Jinping took the lead in charge of the management of network information security in various fields in China. The leading group studies and formulates China's cyberspace strategy to enhance China's cyberspace development capability and the governance voice of international cyberspace.

In November 2016, the Standing Committee of the National People's Congress voted to pass the network security law of the people's Republic of China, This is the first legal practice of China's initiative on the principle of cyberspace sovereignty, which clarifies the scope and protection system of key information infrastructure in cyberspace, and provides a legal text for China to participate in international cyberspace competition and governance. In December of the same year, National cyberspace security strategy released for the first time. The strategy clarified China's major positions and propositions on Cyberspace Security and development, clarified the focus and major measures of cyberspace governance in China in the future, reaffirmed China's determination to firmly safeguard national cyberspace sovereignty and security, and demonstrated China's attitude and responsibility to actively participate in cyberspace international governance. In March 2017, China released the cyberspace international cooperation strategy, the strategy further improved the top-level design of cyberspace governance in China, clarified the basic position, strategic tasks and action plans of China's participation in cyberspace international cooperation, put forward China's plan for international cyberspace governance and contributed China's wisdom to the construction of a common destiny of cyberspace. “One law and two strategies" both show that the core of China's cyberspace strategy is to maintain national cyberspace sovereignty and cybersecurity, actively participate in international cooperation and governance of cyberspace, and advocate the establishment of a democratic, multilateral, fair and transparent global cyberspace governance system.

It can be seen that the idea of active defense runs through the development process of China's cyberspace strategy. China's primary goal is to maintain its own network security, while respecting other countries' network sovereignty. China stands for the establishment of a "community of shared destiny" in cyberspace and the creation of a pattern of international cooperation in cyberspace that "you have me and I have you".

3.2 Evaluate Defensive Cyberspace Strategy

The defensive cyberspace strategy has been adopted by China, Russia and other developing cyberspace powers. Based on their own network strength and clear positioning of cyberspace's international status, these countries respond to the Internet hegemonism by defense, reduce the harm of cybercrime by defense, and build a clean domestic network society by defense. At the same time, it is a positive signal released by the network developing countries represented by China and Russia. It is a country that aims to gather together to seek Cyberspace Security, peace, openness, innovation and shared development. Enhance the voice and influence of developing countries in cyberspace and change the unfavorable situation that the developed countries control the rule making power in international cyberspace governance.

However, under the influence of the actual national network strength and limited discourse power, the main focus of the defensive cyberspace strategy is to maintain the national security and national interests of developing countries, failing to effectively transform the strength of developing countries in the traditional international political competition into the game chips of cyberspace. At the same time, the fact that the network developing countries are growing up is reflected in the network space, which makes the network developed countries feel an urgent threat, so that the network developed countries have stepped up the containment of the network developing countries and the seizing of the network information resources. It can be seen that the defensive cyberspace strategy can only be a one-time strategy for China, Russia and other countries. It is difficult for China, Russia and other countries to break out of the encirclement of the joint clamp down of the network developed countries and obtain the network data resources and network governance discourse right matching their development. The urgent task for developing countries is to realize the independence of key information technologies in cyberspace, create opportunities and platforms for equal dialogue with developed countries, speed up the narrowing of the "digital divide", promote the establishment and improvement of equal, safe, transparent and innovative international network governance mechanisms, highlight the improvement of key information technologies in defense strategies, so as to improve the coordinated defense ability.

4. DEPENDENT CYBERSPACE STRATEGY: LIMITED POWER AND ABILITY OF INDEPENDENT GOVERNANCE

"Cyber colonialism is the concrete manifestation of neocolonialism on the Internet, and also the concrete embodiment of the soft power and smart power of the United States." In the era of globalization, every country is actively or passively involved in various topics of cyberspace development. The network developed countries led by the United States also extended the colonialism in the traditional international politics to the cyberspace. The United States even used its inherent technological advantages to intensify the resource plunder and sovereignty control over other countries. The objective reality that the key information technology level of the network underdeveloped countries is relatively backward makes them have to choose to rely on the network developed countries when making the national cyberspace strategy, so as to obtain time and support for their own economic development.

4.1 Typical Representative of Dependent Cyberspace Strategy: Network Less Developed Countries

In recent years, the network less developed countries have realized that the rapid development of cyberspace has brought them opportunities for economic development and threats to their security. However, due to the weak economic foundation and the late process of national independence, the network infrastructure construction and technical level of the network less developed countries are relatively backward, which forces them to formulate national cyberspace governance strategy with the intervention of Internet developed countries, and even the phenomenon of simply copying the design of internet governance mechanism in western countries, the maintenance of national cyberspace sovereignty is in danger. This is a kind of active dependence under the influence of "positive psychology", ignoring the gap between the network strength and the network developed countries, and reducing the interference of the network developed countries in the real world through the "consistency" of policies, so as to win their economic assistance and support.

On the other hand, the network less developed countries have a wide information industry market and become the "new continent" for Internet giants. Google and Amazon in the United States have been fighting for the development market of African networks. However, due to the more urgent and prominent practical problems in the development of the country, such as ethnic division, epidemic diseases and people's food and clothing, the network less developed countries lack the control and development ability for their own network market. The network infrastructure mostly depends on the network developed or developing countries, and the process of independent development of network information technology is slow, which leads to the emergence of passive dependence.

Its dependent governance strategy is mainly manifested in imitating the network developed countries to formulate the network security governance system, paying attention to the legislative work of fighting against network crime, focusing on economic crime. However, in the actual implementation, due to the limited technology and talents, little effect has been achieved. It is mainly manifested in its participation in the governance of international cyberspace mainly through regional organizations or sub regional organizations, the scope of governance is still limited within its territory, the international discourse power and influence are weak, the relevant conventions formulated are difficult to be recognized by other countries, and more proposals go beyond its actual network governance and law enforcement capabilities. A force that plays an important role in the network governance of the network less developed countries is quite a number of non-governmental organizations, which are supported or controlled by the network developed countries, and become the representative of the western network developed countries headed by the United States in the network less developed countries. In the process of network governance in the underdeveloped countries, this is reflected in the selective "neglect" of American network hegemonism and the squeeze of the development space of their own network sovereignty to obtain some "assistance".

However, in recent years, with the development of economic strength and the increase of network coverage in the network less developed countries, some countries have begun to attach importance to the maintenance of national network security and the development of cyberspace, gradually recognize the hegemonic motivation of the developed countries, start to seek the network technical support from China, Russia and other network developing countries, and establish their own network security governance system, and achieve cross regional network security cooperation.

4.2 Evaluate Dependent Cyberspace Strategy

The dependent cyberspace strategy is not a mature national cyberspace strategy, but a summary of the cyberspace behavior of the network less developed countries, which is a group temporary transition strategy choice.

The network less developed countries have its realistic basis for the choice of the dependent cyberspace strategy. The gap between the less developed countries and other regions or countries can’t be ignored, which is the objective impact of their special national development process. However, it must be noted that the dependent cyberspace strategy can only be used as a plot to gain time in order to complete defense. The network less developed countries should be aware of the "re colonization" trap of cyberspace development. The fairness and justice of cyberspace requires the network less developed countries to attach importance of the independent construction of national network infrastructure, train national network technology talents and establish national network security governance system. As the product of network hegemonism, the dependent network governance strategy covers up the ugly face of the network developed countries, led by the United States, trying to cover up their plundering of data and information resources through the "Marshall Plan" of cyberspace, blurring the fact that cyberspace is polarized and the "digital divide" is expanding. In a word, the dependent network governance strategy has damaged the autonomous power of the network less developed countries and regions to participate in the international network space governance, compressed the space for their network strength to improve, and delayed the opportunity for their network capacity to improve, which will eventually lead to the "re colonization" of the network space.

REFERENCES

[1] C.H.Zhang: Globalization and national sovereignty, nation-state and network colonialism in the Internet Era, Journal of Marxism & Reality,vol.23(2012) No. 4,p.32-41.

[2] Z.B.Hui: Research on Global Cyberspace Information Security Strategy(China Publishing Group, China 2013).

[3] Y.Shen: U.S. National Cyber Security Strategy(Current affairs press,China 2013).

[4] China Academy of Cyberspace.World Internet Development Report 2018(Electronic Industry Press. China 2018).

[5] C.S.Wu: American global strategic public domain anxiety and China's response, Journal of Global Review, vol.34(2014) No. 6,p.90-104.

[6] D.H.Xu: The development of China's information security management in the past 30 years of reform and opening up, Journal of Beijing Institute of Electronic Science and Technology, vol. 22 (2009) No. 1,p. 12-16+11.

[7] C.Y. Lu: Cyberspace Governance and Multi Stakeholder Theory (Current Affairs Press, China 2016).