Discourse Power Construction in the Sino-US Cyberspace Game

Jiayi Kong

Study No.: 20177556

Master's Thesis

Development and International Relations

University of Aalborg, Department of Culture and Global Studies

10th Semester, Spring 2019

Supervisor: Professor Hao Min

Department of International Politics

Date of submission: 15.05.2019

Keystrokes (general text, footnotes, and bibliography): 109,850

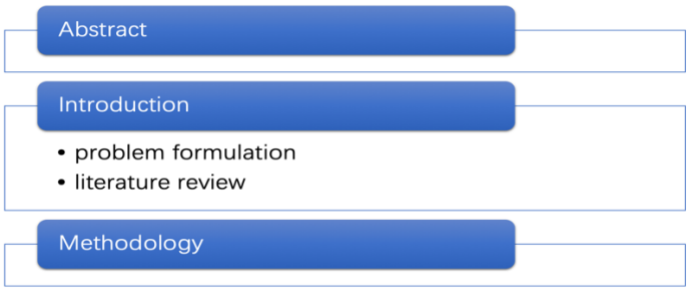
Summary

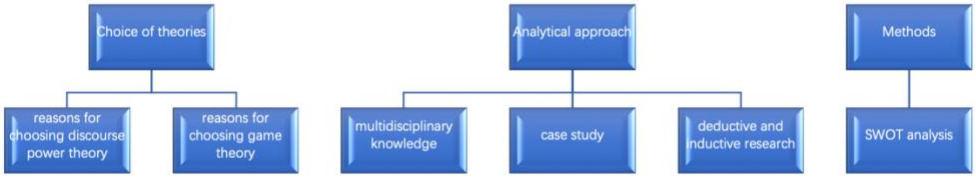
This thesis focus on the Sino-US cyberspace game through analysis of the construction of the cyberspace discourse.

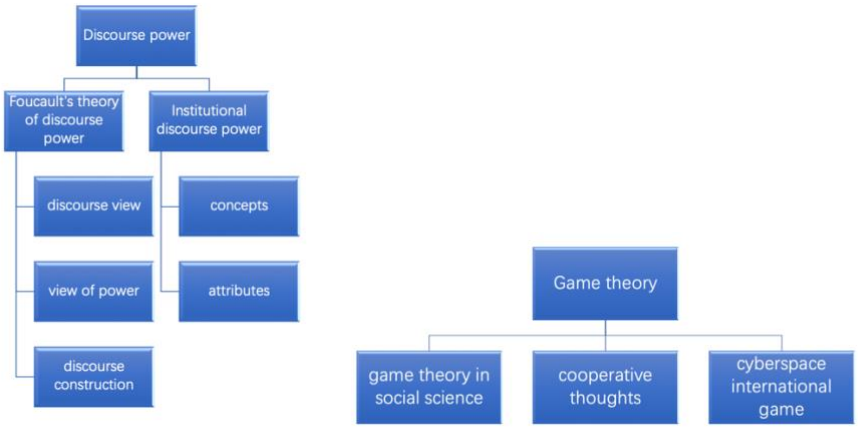
The analytical frame of the thesis is in the following parts. Three analytical approaches multidisciplinary knowledge for analysis and argumentation, case study, deductive and inductive research, and one evaluation method SWOT analysis method are applied in this the methodology part. Theories utilized in this thesis are discourse power theory and game theory. Because the cases analyzed in this thesis is the Sino-US cyberspace game, the construction of cyberspace discourse mainly focuses on Foucault's discourse view and China's new theory of institutional discourse power. There are two parts in the analysis chapter which echo the discourse theory: from the US aspect: the US cybersecurity discourse construction logic, the US cyber discourse hegemony, and construction method; from China aspect: the SWOT analysis of global cyber governance and China's path to institutional cyberspace discourse. The game theory is utilized in the analyzing part of Sino-US game.

After researching and analyzing, the thesis comes to the conclusion that the three main disagreements and different understandings of cyberspace discourse construction which make the Sino-US cyberspace game into cooperation and non-cooperation. China and the United States have principled differences in the construction of the cyberspace governance system. This principled disagreement is structurally different and difficult to reconcile. The core principle of the US cyberspace governance system is "to adhere to the free mobility of information," which is an inevitable continuation of the "Internet openness" in the United States. It means that the United States insists that the free flow of information is the universal "human rights freedom" that the United States wants to universalize. While China promotes the cyber sovereignty which is government leaded. Due to different governance principles, China and the United States have chosen different governance models. the United States believes that the governance of source code and physical technology layers should be placed in a "multi-stakeholder" model, while the governance of online content is

more related to political content.







Content

1. Abstract

Cyber power is playing a more and more important role in international relations. The Sino-US cyberspace game reflects by the dynamic cybersecurity behaviors, the hegemonic adherence to the applicability of the US cyber hegemony, and the discourse construction of both China and the US. Foucault's discourse theory describes the certain system under historical conditions, which to be used in the big data era, the discourse construction is introduced into cyber power of countries. By the classification of interactive nature of games theory, the cyberspace game between players -- China and the US is dynamic, both cooperative and non-cooperative, and strategic macro. The cyberspace discourse power is a main factor in the Sino-US cyber game. The US constructed its cyber discourse by institutional methods, hegemonic status, and legitimacy influence. The technic barriers is one of the key factor using in the game with China. China's strategic choice includes interfering more into global governance, constructing institutional voice, promoting globalization, and building international institutions.

Key Words

Cyberspace, discourse power, game, international relations.

2. Introduction

2.1. Problem formulation

How does discourse power construction and disagreement between China and the US influence the Sino-US cyberspace game?

2.2. Literature review

Some scholars recognize that national sovereignty and national security are being challenged by the cyber era, and the evaluation standards of national power are also changing. But their power to cope with these challenges in the era of cyber continues. It is

optimistic for big countries to strengthen the countrys' power and consolidate their leading positions. For example, WIlenstein believes that liberalism is the ideology of the capitalist world system, and it always guarantees the accumulation process of capitalism and the process of distribution of surplus value. The representative ideas in this aspect are: Josephs Nye's "America's Information Edge" and "The Power of Information"[1], Andrei Krutskikh and Galina Kramarenko's from Russian Ministry of Foreign Affairs Security "Diplomacy and the Information Revolution"[2], David J. Rothkopt's "The Changing Nature of Power in the Information Age"[3], and etc. In their views, the issue of defending national security and international security is showing a fundamentally different aspect in the context of the rapid expansion of ICTs. The information resources of the entire country have become the most powerful information weapon attacks in malicious attacks or information warfare. The great potential of Internet information technology has become an important tool for countries to seek political and military hegemony on the international stage.

Scholars have conducted in-depth and comprehensive research on warfare in the cyber age. One type of research is mainly from the military science and technology sector. For example, the American Silicon Valley scholar Xiao Zong analyzes the war in the cyber age in detail. He believes that the factors of time in the cyber age are more prominent, and the material flow and energy flow in the war are unified in the overall planning and leading of information flow[4]. Through reconnaissance satellites, warning aircraft, optical cable eavesdropping on the seabed, long-range radar on land, and port scanning on the internet, the two sides of the confrontation are all collecting, capturing, transmitting, processing, and analyzing. Information has risen from the supporting role of the war in the past to the main role. The information warfare competition in the cyber era is no longer human and material resources, but the human intelligence to grasp the information superiority.

---

[1] Joseph S. Nye, *Bookshelf: The Power of Information*, Wall Street Journal, 10 September 1992.
[2] Andrei Krutskikh, Galina Kramarenko (2003), *Diplomacy and the Information Revolution*, International Affairs, Vol 49, No. 5, p. 116.
[3] David J. Rothkopf (1998), *Cyberpolitik: The Changing Nature of Power in the Information Age*, Journal of International Affairs, Vol 51, No. 2, p. 345.
[4] Xiao Zong, 《信息安全与信息战》, Tsinghua University, 2003, p. 7-8.

Another type of research comes from the social science field, mainly from the study of international relations scholars. For example, Swedish scholar Johan Eriksson and Italian scholar Giampiero Giacomello provide a new perspective for us to understand the concepts of cyber threats and cyber warfare from the perspective of constructivism. In their paper "The Information Revolution, Security, and International Relations: (IR)Relevant Theory?", they believe that the private sector or the public sector are aware of cyber threats, but this perception is different for the military sector and the public[5]. The prominent image of cyber threats within the business community and the police department is cybercrime; for the bureaucracy, the image of the cyber threat is the Information War (IW), information action (Information Operation, IO), cyber terrorism, and cyber warfare; for technologists, their image of cyber threats is mainly cyberattacks, improper use, or network damage[6]. Although there are different opponents and targets in different perceptions, the country is still regarded as the most important potential adversary to destroy the critical infrastructure of other countries.

3. Methodology

3.1. Choice of theories

This thesis chose the theory of discourse power and game theory from the perspective of constructivism.

3.1.1. Reasons for choosing discourse power theory

From the perspective of constructivism, discourse is not only a reaction to reality, but also

[5] Johan Eriksson, Giampiero Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)Relevant Theory?*, International Political Science Review, Vol 27, No. 3, p. 221—244.
[6] Johan Eriksson, Giampiero Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)Relevant Theory?*, International Political Science Review, Vol 27, No. 3, p. 227.

a social practice that influences, constructs, and produces reality. According to the securitization theory of the Copenhagen School in International Relations, the security issue itself is a subjective construction process as a discourse act[7]. Therefore, in recent years, more and more research has begun to explore the construction of discourse and its impact in cybersecurity. Specifically, this thesis will use a quantitative content framework analysis and qualitative discourse analysis from the perspective of constructivism.

In the analysis of the construction of discourse power in cyberspace, this thesis adopts Michel Foucault's discourse power theory and China's Institutional Discourse Power concept.

From the "unipolar moment" to the "unipolar era", the United States played an important role in the discourse constraints of the challenged countries[8]. The arrival of information technology has changed the social structure, made society and government more dependent on information technology and vulnerable to various network threats. Therefore, the United States, which adheres to the hegemonic concept, has begun to attach importance to constructing a discourse institution to deal with cyber threats and cyber terrorism. The concept of cyber threats is partly the result of the transition from an industrial society to an information society. It is also a fertility of subjective fears that arises from increased vulnerability and loss of control. At the same time, the United States promotes its international policy in the field of cyber security with asymmetric power, plays the role of an interpreter of the new phenomenon of the network, and adopts the “preemptor principle” in the construction of cyberspace discourse[9]. This paper will analyze how the United States constructs cybersecurity discourse power, summarize the thinking logic that supports its constructive behavior, the internal institutionalism of US cybersecurity discourse construction, and the externalization process of hegemonic construction. On this basis, the thesis will discuss the construction strategy of Chinese cybersecurity discourse.

---

[7] Ole Wæver (2011), *Politics, Security, Theory*, Security Dialogue, Vol 42, No. 4–5, p. 465–480. https://doi.org/10.1177/0967010611418718

[8] Yuan Sha (2017), *Discourse Checks and Balances Hegemonic Protection*, World Economics and Politics, No. 3, p. 85-107.

[9] Shen Yi (2014), *Global Cyberspace Governance and BRICS Cooperation,* International Watch, No. 4, p. 145-157.

The concept of "institutional discourse power" is a new concept put forward by Chinese President Xi Jinping on promoting China's comprehensive and in-depth participation in global governance. It refers to a country's participation in international institutionalisms, through agenda setting, norm shaping, rulemaking, and initiative mobilization. And the way in which institutional ideas spread, influence the design and operation of international institutionalisms, to seek China’s own initiative or dominance in international institutionalisms, and internationalize and legitimize China’s policy discourse. This theory can analyze China's participation in the construction of global cyber security governance from the perspective of the rise of socialism with Chinese characteristics and the rise of great powers.

3.1.2. Reasons for choosing game theory

The game theory from mathematics and economics field has been used and developed rapidly in international security and international political economics since the 1950s. With the help of game theory, realists made powerful strategic analysis and theoretical deductions on the conflict and confrontation between big powers in the 1960s and 1970s. The liberals applied it on the issue of state cooperation in the 1980s. As an important part of the scientific method, game theory plays an important role in promoting the scientific process of the international relations discipline.

The development and popularization of the Internet has made more and more abundant types of actors involved in international interactions. The states face opportunities and challenges in this process to protect national security and interests. The basic types and characteristics of the international game of the cyberspace, and the status of the actors involved in it are the basic problems in the study of the interactions of contemporary international relations. The use of game theory in cyberspace can analyze these basic problems and help us to explore the law, recognize the trend, and grasp the competitions and cooperation in the interactions of any international relations in the contemporary complex game and cooperation situation.

3.2. Analytical approach

First, multidisciplinary knowledge for analysis and argumentation is comprehensively utilized in this thesis. The international game and cooperation of the Internet involves all aspects of international relations such as politics, economy, culture, science and technology, and military. It requires the comprehensive use of political science, international political economics, network economics, international law, sociology, military science, and computer science. Such subject knowledge, comprehensively examine and analyze the problem from different academic backgrounds.

Second, case study method is used comprehensively. This thesis presents the urgency of the current cyber space international game and the fierce situation in the cooperation process. The objects are developed countries which is represented by the US, the difficulties faced by developing countries as China, and the strengthening of cooperation games to solve the increasingly serious global cyber security problems. The thesis pays attention to the use of newer cases to demonstrate this process. At the same time, the scientific case selection tries to overcome the unfavorable factors such as small sample size and large randomness in case study, and maintain the consistency or similarity of the selected positive and negative groups, which can enhance the persuasiveness of case study methods by comparing differences.

Third, deductive and inductive research methods are applied. The deductive path is usually based on the existing literature and then test these frameworks. The inductive path has no specific pre-defined framework, the purpose of which is to identify all possible frameworks from the data itself, so a framework based on specific issues is proposed. Each of the two paths has its own advantages: the general framework under the deductive path tends to help to transcend the construction theory of a particular topic; the specific topic of the inductive path is useful for revealing the unique characteristics of a particular issue. For the purposes of this thesis, it combines top-down deduction and bottom-up induction. From the perspective of deduction, this thesis analyzes the meaning and influence of the game in cyberspace from the three levels: the US cyberspace discourse power construction,

China cyberspace governance, and Sino-US cyberspace game. From the perspective of inductiveness, through the specific demonstration and analysis of the Internet international game and cooperation issues at various levels and in different fields, this thesis analyzes imbalances on the survival and discourse of countries and the international game.

If quantitative-based framework analysis focuses on systematic presentation of discourse features, then qualitative discourse analysis aims to deepen the understanding of discourse generation and more complex social power relations. The analysis focuses not only on the discourse framework itself, but on revealing deeper international relations and power imbalances behind the discourse. This aspect echoes the perspective of constructivism theory, which regards discourse as a specific social practice and is linked to social situations, organizations, and institutions. On the other hand, critical discourse analysis is also in line with the development of cybersecurity in China. The discourse construction of cybersecurity is constantly evolving with technological development, social change and, Sino-US relations.

3.3. Methods

To evaluate China's national conditions and the world's cyber space game, this thesis uses the SWOT analysis method in strategic management to analyze the internal and external conditions of China's participation in global cyber governance.

SWOT analysis, also known as situational analysis, is an analytical framework that is widely used in strategic management processes and is often used to develop corporate development strategies. SWOT refers to Strengths, Weaknesses, Opportunities, and Threats. Among them, advantages and disadvantages refer to internal factors of actors, and opportunities and threats refer to objective factors in the external environment that are beneficial or unfavorable to actors.

SWOT analysis is simple and applicable. When conducting strategic analysis and evaluation from the perspective of SWOT analysis, the internal and external factors of the actor should be comprehensively analyzed and arranged according to the degree of

influence and urgency. In theory, according to the principle of two-two combination, the strategic decision through the method includes four kinds: Advantage + Opportunity Strategy (SO), Disadvantage + Opportunity Strategy (WO), Advantage + Threat Strategy (ST), Disadvantage + Threat Strategy (WT). In several models, the SO strategy that emphasizes the advantages and opportunities is an ideal strategy; the WO strategy emphasizes the use of opportunities and compensates for disadvantages; the ST strategy emphasizes the use of advantages and avoids threats; the WT strategy emphasizes the elimination of disadvantages and the elimination of threats. For national actors, this definition is largely interlinked. SWOT analysis methods are equally applicable to China's participation in global cyberspace governance.

4. Theories

4.1. Discourse power

4.1.1. Foucault's theory of discourse power

Michel Foucault (1926-1984) was a philosopher who transitioned from structuralism to deconstruction in the 20th century. Based on the critical inheritance of modernism, Nietzsche and his philosophy, and structuralism, he put forward the viewpoint of "discourse is power" and formed the theory of discourse power. He published The Order of Discourse and Discipline and Punishment in the 1970s with the viewpoint of "discourse as power". However, in the period of power genealogy, Foucault gave up the self-discipline of discourse. He introduced power into the analysis of discourse and formed a unique theory of discourse power theory. He believed that discourse and power are inseparable, power generates discourse, and discourse in turn generates power. The two interact and support each other and jointly promote the development and progress of society.

4.1.1.1. Foucault's "discourse" view

Foucault's concept statement described in *The Order of Things* is the basis for understanding the concept of "discourse"[10]. In Foucault's own words, discourse refers to a group of statements that are "supported by a certain system under certain historical conditions". For the "statement", Foucault also explained from a negative perspective: first, the statement is not a sentence, therefore, it is not subject to specific grammatical rules, an equation, a book, a chart, or a growth curve, these are not related to grammar; second, the statement is not a proposition, therefore, it is not subject to the control of specific logic rules; finally, the statement is not a specific speech act, the speech act is composed of multiple statement constitutes. Foucault pointed out that the statement is only a function of the tool. Foucault believed the meaning, definition and what is meant by the statement is irrelevant. The statement is not a unit with a definition but only a tool for discourse analysis. Therefore, it is only possible to understand the statement based on the function of the statement.

4.1.1.2. Foucault's view of "power"

In 1970, Foucault introduced power into discourse analysis. He pointed out in his book The Archaeology of Knowledge that in every society, the production of discourse is controlled, selected, organized, and redistributed according to a certain number of procedures[11]. The function of these programs is to eliminate the power and danger of discourse, to deal with accidents, and to avoid its heavy and terrifying materiality.

What is power? Foucault believes power is not an institution, not a structure, nor a power. It is just the name people use for complex strategic situations in a particular society. Overall, from Foucault's theory, power has the following characteristics.

(1) Power is "non-central". For a long time, people thought that the ruling class, the state,

[10] Michel Foucault (1994), *The Order of Things*, Reissue.

[11] Michel Foucault(1969), *The Archaeology of Knowledge,* Random House USA Inc, New York, United States.

and the law are the representatives of power. Therefore, the revolution must also start from these aspects, as long as the ruling class is overthrown and subverted. In Foucault's view, this traditional view of power does not really recognize power. In fact, before the country was born, power existed. It existed as a kind of power relationship and existed as a political technology that dominated people. Any node in the power network can be called a power center. Foucault promoted to seize and study the most regional and most partial power in the form and system[12]. In Foucault's view, the state and the ruling class cannot be the target of struggle, so that they cannot truly resist power. There is no centrality of large-scale rejection, the core of rebellion, the root of all betrayal, or the pure law of revolution. On the contrary, there are only pluralistic resistances, each of which is a special case.[13]

(2) Power is non-main. Foucault believed that everything can be concluded into two things: power and discourse. They are mutually constructive and together contribute to the formation and development of society. The subject is nothing but a tool constructed by the discourse relationship network. Transcendental, independent subjects do not exist. They are only products that are passively constructed by power. "In fact, the body, manners, words, and desires are identified and constructed as individuals which is the initial result of power[14]. Therefore, the key to understand power is not to explore who is the master of power, but to study the institution by which power operates and how discourse is formed in this power institution. Foucault pointed out that our main task is to discover how the subject is constructed by the power institution, and how the discourse is formed in this power institution, so that we can find ways and means to resist power.

In summary, in Foucault's view, “discourse” is inseparable from “power”. In the process of formation and development, it has always been controlled and disciplined by “power” and competitions in specific power fields. The battle for people's discourse is actually aiming for power. Power controls the discourse, while discourse is constantly producing and strengthening power.

---

[12] Michel Foucault (1999), *Society Must Be Defended*. Abnormal, p 23-26.
[13] Steven Best, Douglas Kellner(1997), *Postmodern Theory*, The Postmodern Turn.
[14] Michel Foucault (1989), *Foucault Live: Interview*, Semiotext New York, p. 210.

The emergence of the Internet has made the using of power more and more secretive, and people have unwittingly accepted the norms and constraints of power. It is like a big net, which regulates people's acts. As the birthplace of the Internet, the United States has the irreplaceable technical and institutional advantages, and it has the supreme discourse in cyberspace. Exploring how power works through the Internet to give the United States a cyberspace discourse hegemony is a method to understand the construction of cyberspace discourse.

4.1.1.3. Discourse construction

"Discourse construction" is a very important concept in Foucault's academic field. In Foucault's view, the entire civilization of mankind, whether brilliant or dark, whether it is great or small, is a kind of construction. The entire human history is a history of self-construction about human beings. In these constructions, the most basic and most important construction is the “discourse construction”.

Discourse is a platform for communication and understanding between human society. It is because of the platform of discourse that human beings can construct various systems, laws, principles, powers and even civilizations on this basis. Therefore, it can be said that “discourse” is the most initial and most important construction. At the same time of discourse construction, it is constantly deconstructed and reconstructed in the long human history, so the entire discourse history is extremely complicated. It is precisely because of the constant construction, alternation, deconstruction, and reconstruction of discourse that discourse has constantly constructed a variety of infiltrating powers in history, and power in turn constructs new discourses as power. Discourse of service; discourse constructs the whole history. It can be said that human beings or ridiculous or great historical civilizations are constructed by discourse. History does not have the truth or illusion. Therefore, Foucault in the book The Archaeology of Knowledge tirelessly depicts that "the history of knowledge is composed of basically intermittent historical periods with different cognitive

characteristics.[15]"

Discourse is a sociocultural code that has been formed through a long period of historical accumulation. The form of verbal words potentially restricts people's thoughts and behaviors. Once the discourse is formed, it has its own meaning world, forms its own specific rules, and builds its own knowledge form and discourse system. The language is artificial, and the language also creates civilization.

4.1.2. Institutional discourse power

The "institutional discourse power" is a new concept put forward by Chinese President Xi Jinping on promoting China's comprehensive and in-depth participation in global governance. In July 2014, when Xi Jinping visited Brazil, he first proposed that the BRICS countries should strengthen cooperation and strive for more institutional power and discourse in the global governance of developing countries. In October 2015, the 18th CPC Central Committee pointed out that China will actively participate in global economic governance and supply of public goods, improve China's discourse in global economic governance, and build a broad community of interests." In November 2015, the CPC's Thirteenth Five-Year Plan for Social Development further pointed out that China should actively participate in the development of international rules in international cyberspace, the deep sea, the polar regions, and the sky. In October 2016, in the Political Bureau of the CPC Central Committee, the new goal of "accelerating the promotion of China's right to international discourse and rulemaking in cyberspace" was put forward by Xi Jinping.

4.1.2.1. Concepts of institutional discourse power

The institutional discourse power refers to the influence of a country's participation in the international institution, through the setting of the agenda, normative shaping, rulemaking, initiative mobilization and the dissemination of institutional ideas, to influence the design and operation of international institutions. It aims to be initiative or dominance in the

[15] Michel Foucault, *The Archaeology of Knowledg*e, Gallimard; GALLIMARD edition (February 7, 2008)

international institution, to seek the power to internationalize and legalize domestic policy discourse. In essence, institutional discourse power pursues the influence of a country's policy discourse and is based on "rights." The power of institutional discourse is given by international institutions, but the key is not the international rules and institutions themselves, but who sets the rules and who the rules represent, whether they are “passively obeying the rules” or “proactively making rules”.

4.1.2.2. Attributes of institutional discourse power

First, the complexity of the composition. Institutional discourse power is not a singular concept, but the collision of many concepts and rules. The complexity of institutional discourse power can be understood from both theoretical and practical dimensions. In theory, institutional discourse power is a compound power, the core concepts of international relations, such as "power", "institution", "discourse", the important theme of "discourse", "order", and discourse politics. The connection and interaction between “identity”. In reality, with the specialization of the international system, the refinement of the field, and the imitation and spillover of the organization[16], the international system is chaotic, the number of international organizations has soared, the parallel system has emerged, and overlap.

Second, the indirectness of expression. Institutional discourse power is an indirect power that subtly shapes international behavior with the procedural rationality and contractual spirit of the international system. The indirectness of institutional discourse power is reflected in three aspects: first, it works through a specific carrier. Institutional discourse power is not automatically generated by actors, but is subject to the effectiveness of institutionalized carriers such as international law, international treaties and international declarations. Second, institutional discourse power is not self-construction in a conventional environment, but is generated and disseminated in multilateral or bilateral international situations such as international organizations, international conferences, and

[16] Wu Zhicheng, Dong Zhuangzhuang (2016), *International System Transformation and China's Response*, Contemporary World, No. 5, p. 11

leaders' meetings. The third is the necessary steps to be legalized. The institutional discourse power is not the direct transmission of international power between the actor and the receiver, but is to be perceived in a more rational and standardized way through the processing and confirmation process.

Third, the diversity of content. Institutional discourse power has multiple aspects, and its content is very extensive. In terms of the nature of power, institutional discourse rights include both “hard powers” generated by formal international institutions such as international law, international treaties, and international agreements, as well as “soft power” generated by informal international institutions. In terms of the main areas involved, institutional discourse rights cover both the “high-level political” field of international relations such as politics and security, as well as the “low-level politics” of international relations such as economics, society, science and technology, and culture.

4.2. Game Theory

4.2.1. Game theory in social science

Game theory was originally an ancient thinking game that was officially used for scientific analysis since the 20th century. In 1928, mathematician John Von Neumann founded the two-person zero-sum game. In 1944, Oskar Morgenstem apply his game theory into economic analysis with the book Game Theory and Economic Behavior. In 1950, mathematician John F. Nash promoted Nash equilibrium, which improved game theory from zero-sum game to non-zero-sum game, enabled it to be more widely used to daily life analysis. In the same year, A. W. Tucker defined the “Prisoner's Dilemma”. Their work laid the cornerstone of modern non-cooperative game theory. Since then, the study of game theory has been further refined and extended. In 1965, Reinhard Selten cites dynamic analysis and proposes the concept of “refined Nash equilibrium”. In 1967, John C. Harsanyi introduced incomplete information into the study of game theory. D. Kreps and R Wilson collaborated in 1982 to publish important articles on dynamic incomplete information. In this way, four game analysis models are formed in the informal cooperation game theory,

which are complete information static game (Nash equilibrium), complete information dynamic game (subgame refined Nash equilibrium), no safety information static game (Bayer Snash equilibrium), and incomplete information dynamic game (refined Bayesian Nash equilibrium).

There are many types of games. This thesis uses the classification of interactive nature which divided games into cooperative games and non-cooperative games. The difference between them is whether the game can reach a binding agreement.

4.2.2. International game theory and cooperative thoughts in international institutionalism theory

The theory of neo-realistic international institutionalism and the theory of neo-liberal international institutionalism are two rationalist schools of international institutionalism theory[17].

The theory of hegemonic stability is the most authoritative and universally accepted interpretation of the institutionalism by the new realism[18]. The basic idea is: hegemonic powers establish a hegemonic system, and establish basic principles, rules, norms, and decision-making procedures within the hegemonic system. The premise of other countries accepting these international institutionalisms is the strength of hegemonic states. Second, hegemonic states can obtain the maximum benefit. At the same time, hegemonic states provide the public goods generated by these international institutionalisms to the rest of the system in order to maintain the system and its own interests. Hegemonic states are tolerant for Free-rider. This international institutionalism will change accordingly as the status of the hegemonic power changes.

---

[17] Andreas Hasenclever, Peter Mayerand Volker Rittberger (1997), *Theories of International Regimes*, London: Cambridge University Press, p. 1-2.

[18] Robert Crawford (1996), *Regime Theory in the Post-Cold War World: Rethingking Neoliberal Approaches to International Relations*, Dartmouth: Darmouth Publishing Company, p. 57.

At the same time, the institutionalism itself can in turn become the basis for power enhancement or the source of power generation[19]. This leads to the fact that the international actors, and even after the establishment of the institutionalism will continue to play a fierce game. For example, with the global popularity of the Internet, the relevant systems for the global use, maintenance, and management of the cyberspace have become the targets of various international actors, including countries, especially large countries. As the birthplace of the Internet, the United States has a first-mover advantage. It has initiated a series of international organizations to formulate and improve relevant systems, and to share the requirements for sharing cyberspace discourse of other countries and international actors. Such actions further maintained and expanded their national interests through international institutionalisms.

It can be seen that the theory of international institutionalism draws a lot of contents from game theory. Like game theory, it focuses on the issue of competition and cooperation under anarchy, including important issues such as hegemony, relative income, and interdependence[20]. The interactive processes and models in the international political, economic, scientific, cultural, military and other relations will show the characteristics of certain games. "All the states are trying to find out the other's intentions and in the process of development with the current situation.[21]" Game, game theory, bargaining, and decision-making have strong correlation with international relations research. However, what we call international game and cooperation does not refer to a specific meaning in the sense of the interaction of abstract international relations, but a macro-strategic game and cooperation. Game theory is only one of the important tools for analyzing international games and cooperation, especially for specific problems. International game and cooperation are more emphasis on understanding the overall international relationship from the perspective of the game method and perspective. In this sense, we can also abstract the entire international relationship, including international games and cooperation

[19] Stephen Krasner (1985), Structural Conflict: *The Third World Against Global Liberalism*, Berkelay: University of California Press, p. 7-9.
[20] Andrew Kydd and Duncan Snidal (1993), *Progress in Game-Theoritical Analysis of International Regimes, in Volker Rittberger (ed.)*, Regime Theory and International Relations, Oxford: Clarendon Press, p. 112.
[21] Kenneth Neal Waltz, Waveland Press; 1 edition (February 5, 2010), p. 150

into a mixture of zero-sum games and non-zero-sum games in which multiple actors participate.

4.2.3. Cyberspace international game

On the one hand, the global spread of the Internet has contributed to the increase in the number and strength of non-state actors, new interest groups and political groups have emerged, and their claims and demands have made the international game, which was originally fiercely competitive, even more rigorous. Joseph Nye discussed the distribution of power in the age of information age in Redefining NATO Mission in the Information Age [22]. He believes that contemporary power distribution is like a three-dimensional game. From a military perspective, the unipolar is obvious, and the US's advantage clearly exceeds that of all other countries, which its military expenditure is even larger than the sum of the expenditures of the eight countries that follow. The United States is also the leader of the new military revolution in the information age and the only country with intercontinental missiles and global deployment of sea, land and air forces. From the economic perspective, it presents a multi-polar pattern with the United States, Europe, and Japan, occupying two-thirds of the world's production. However, in the perspective of the cross-border relationship composed of non-state actors, its power structure is more dispersed. The background of the information age and the complexity of the resulting power structure make the main players of international games and cooperation become more difficult for countries to formulate strategies and policies, because it means competing in several dimensions simultaneously. Therefore, facing the new threats and challenges in the information age, modern countries, hegemony, in order to maintain their original advantages, nationalism and conservative sentiment may re-emerge, "national networks will become part of the emerging networks of the world.[23] " Moreover, the information revolution has not fundamentally shaken the advantages of state actors, especially for big powers. The decline on the surface of modern state power is simply

[22] Joseph S. Nye, Jr. (1999), *Redefining NATO Mission in the Information Age*, NATO Review, Vol 47, No. 4, p. 12.
[23] John Naisbitt, *Megatrends Asia: the Eight Asian Megatrends that are Changing the World*, Nicholas Brealey, 1995.

because it has not yet been able to adapt to the challenges of the information revolution in time. Robert Keohane and Joseph Nye believe that the reason why the information revolution did not transform world politics into a completely complex and interdependent new world politics is that information does not flow in a vacuum, but in politics that has been occupied by various traditional forces[24]. This means when the old international system is transformed into a new stage by the new technologies, the original hegemonic countries and interest groups will try their best to maintain their status and advantages. Conservative thinking will rise, and competition for cyber and information will be inevitable in the Internet information age. In the intangible "information domain", the West are using their economic and technological advantages to expand the dissemination and influence of information, which will inevitably lead to opposition and resistance from other countries. To a certain extent, this will undoubtedly increase the competition and confliction in international games and cooperation.

Due to the Internet's super-embedding and penetration capabilities into the global society, the Internet has become a new global geospatial space[25]. The international political, military, economic, technological, and cultural games and cooperation have not been able to go completely apart from the Internet environment. In quite a few cases, the Internet has directly become a strategic tool and means for all kinds of games and cooperations.

The extensive coverage of the Internet and global connectivity have made information more important, but also made information from the supporting role of war into a protagonist[26]. From the beginning of historically recorded human conflicts, new technologies and always the key to breaking the balance of power. War horses, bows, armor, gunpowder, ship vanadium, steam engine, submarine, air force, nuclear weapons and space weapons have been introduced to the battlefield, and immediately changed the power contrast. The party with these new technologies and new crafts has the ability to defeat in confrontation. For these reasons, the military is often the sector most interested

[24] Robert O. Keohane, Joseph S. Nye Jr. (1998), *Tower and Interdependence in the Information Age*, Foreign fairs, Vol 77, No. 5, p.84.
[25] PCCIP: *President's Commission on Critical Infrastructure Protection.* At http://www.info-sec.com/pccip/web/backgrd.html. (accessed on 20/06/2002)
[26] Xiaozong (2003), *Information Security and Information Warfare*, Tsinghua University Press, p. 12.

in technological innovation. The current Internet has gradually transitioned to a wireless network that is both invisible and ubiquitous. The network serves as the basic environment for the operation of contemporary information warfare, the impacts are: first, the nation-state or group has increased communication in handling international security affairs. The platform improved the understanding and people's public opinion. The possibility of vicious confrontation events, including internet information warfare has been reduced in international games and cooperation. Second, non-state actors armed by the Internet have also increased the possibility of using the Internet to launch information warfare. Third, compared with the traditional nuclear deterrent, the cyber attack deterrence is becoming a reality. ICTS technology that collects, processes, screens, and accurately destroys targets from a distance is more conducive to attack than defense. At present, the US Army and Navy have now formed information warfare units, and can use computers as an offensive weapon in an imposing manner[27]. They have the ability to enter the enemy's computer-controlled national infrastructure through public networks to heck critical facilities such as power grids, telephone systems or satellite systems[28]. Computer-controlled, high-performance laser transmitters can even aim and hit satellites around the earth. Therefore, even if the world is closely linked by the Internet and relies on the ever-increasing contemporary, the importance of military forces in safeguarding national security and safeguarding national development is unquestionable. The competition and conflict of international military games and cooperation are in information. The cyber era will have new performances. Taking the possibility of privatization of war into account, the global military game and cooperation will be more complicated, and the country must not only face traditional opponents, but also face other Non-state actors. On the other hand, there are many common interests among countries in preventing non-state actors from maliciously attacking global critical infrastructure, thus it will be possible to maintain a certain degree of communication and cooperation among states.

---

[27] *The "Future of Warfare"*, Economist, 8 March 1997. at http: www.economist.com/tfs/archive-trameset.html. (accessed on 11/01/2009).

[28] David J. Rothkopf (1998), *Cyberpolitik: The Changing Nature of Power in the Information Age*, Journal of International Ajfairs, Vol 51, No. 2, p. 344.

5. Analysis

5.1. The US cyberspace discourse power construction

5.1.1. The construction logic of the US cybersecurity discourse institution

5.1.1.1. Internalization logic of ideas affecting behaviors

In view of the analysis of cybersecurity behavior in the United States, the hegemonic adherence to the concept explains the applicability of the US cyber hegemony. The discourse construction is an important way to hegemonic protection, and the hegemony establishes discourse consensus domestic and international. Alliance to maintain hegemonic status, legitimacy and influence[29]. As Arnold Wolfers pointed out, research security can be both objective which is the existence of a real threat, and subjective, the existence of a perceived threat[30].

Therefore, according to the thinking mode influenced by the concept, the United States can actively realize its own design blueprint in anarchy through a diversified path. In the cyberspace security structure, the United States plays an active and positive shaping role, which is determined by its strength and its historical status. At the same time, the United States continues to follow Hobbes's ideology in accordance with traditional thinking. Countries outside the cyberspace alliance system are regarded as the targets of threats, creating an atmosphere of hostility and cyber fear.

Based on Hobbes culture, there may be an adversary symbiosis and an in-group phenomenon. The concept of adversary exists in the process of cyber security. It refers to

[29] Yuan Sha, *The Balance of Discourse and Hegemony Protection, World Economics and Politics*, No. 3, 2017, p. 85-107.
[30] Arnold Wolfers (1962), *Collective Defence Versus Collective Security,* The Johns Hopkins Press, p.183.

the logic that it is difficult to locate the source of the attack due to the uncertainty of information. The state uses the means of rendering threats to build the enemy of cyberspace. The United States describes the picture of the threat of self-survival to define actions. In recent years, the US media and government-concluded national actors have shaped China as the largest cybersecurity threat of the United States. At the same time, when the United States acts as a network security incident interpreter, it does not distinguish between individual and hacker attacks from government support. Instead, it assumes cyber attacks coming from China as government support.

In response to the inherent unity, the United States relies on dangerous words and exaggerates threats to achieve the goal of not only uniting groups but also wooing private enterprises. On July 30, 2015, the National Broadcasting Corporation (NBC) published an exclusive report: A so-called confidential map claiming to be obtained from the National Security Agency shows that China has launched nearly 700 times against the United States in the past five years. Cyber attacks, targeted by Chinese hackers, cover almost every industry in the US economy, including business giants such as Google and Lockheed Martin, as well as government agencies and military departments. In the end, the US Department of Defense's 2015 Network Strategy listed China as a key country that constitutes a cyber threat, and a focus of cyber operations in the next five years[31].

The identity interests and discourse texts have mutual logic. Michel Foucault's theory about power creating knowledge and role-dominated discourses presuppose that role identities determine the preferences of discourse, while discourse invisibly shape the perception of role identities[32].

First, as the most powerful country in the international system, the United States is regarded as a hegemonic power, and will determine strategic goals and security interests based on the stable role and relationship formed in the international community. Robert O. Keohane used the compound dependence model to explain the decline of American

[31] U.S Department of Defense, *The Department of Defense Cyber Strategy*, https://www.defense.gov/Portals/1/features/2015/0415_ cyber-strategy/Final_2015—DoD_CYBER—STRATEGY—for—web.pdf

[32] Ferdinand de Saussure, Perry Meisel, Haun Saussy, Wade Baskin (2011), *Course in General Linguistics*, New York:Columbia University Press, p.20.

hegemony. He believed that before the US hegemony had completely declined, it would establish an international system that represented the interests of the United States in order to rebuild and restore its hegemonic effectiveness to achieve post-hegemonic cooperation [33]. The hegemonic protection of critical theory is extended to the level of conceptual culture, and it is believed that hegemonic parliament uses discourse practice to maintain cultural status such as knowledge, identity, and concept[34]. In general, the dominant hegemonic country uses its hegemonic advantages to balance discourse, which would extend the scope of implementation from the traditional security field to the non-traditional security field, especially the cyberspace level, in order to maintain the legitimacy of hegemony.

Second, the construction of discourse power will shape and strengthen the role orientation and interest perception among countries, and determine the motivation and bias of interference with relevant countries. At the internal level of the country, discourse has inherent instability, so in times of crisis, there will be confusion and uneasiness in pessimism. At the same time, in situations where the country is politically divided, there will be problems such as lack of cohesion and strategic goals that needs a unified identity discourse to resolve. At the international level, discourse influences the identity and role consensus among countries. Hostile discourse interactions can hinder the identity cognition and undermine trust institutionalisms among nations. For example, as a rising country, China is a hegemonic challenger in the context of a hegemonic power. The political attitude of the hegemonic power is to suppress it, while the discourse bias is a negative criticism. For the alliance, in order to construct a consistent interest perception, the hegemony will adopt an active and friendly discourse bias, while the domestic rulers aim to construct a threat-sharing model to flexibly unite the audience.

[33] Joseph S. Nye, Robert O. Keohane (2011), *Power & Interdependence,* Pearson, 4 edition, p. 40-44

[34] Steven Weber, Bruce Jentleson, The End of Arrogance: America in the Global Competition of Idea, Cambridge: Harvard University Press, 2009, pp.148-160.

5.1.1.2. Cybersecurity spillover logic

Based on the theory of cultural hegemony, Robert Cox pointed out that the hegemonic class in the hegemonic power will control the domestic social or political order and promote it abroad to establish a country when exercising the symbolic power, which can benefit political, economic, and social interest[35].

First, the US technology company's dominance of the Internet economy is a prerequisite for the spillover of US cyber security. The United States accounts for 35% of global telecom revenues and more than 40% of online revenues; in India, the top 25 websites are US websites (such as Google, Facebook, Twitter, Linkedin); more than 50% of the 25 largest websites in Brazil and South Africa It is operated by a US company. Google is a leader in searching field with its Android operating system accounting for three-quarters of the world's smartphones[36]. At the same time, the structure of the Internet has brought great appeal to the United States.

Second, based on strong hard power and soft power, the United States spills the logic of geopolitics into the cyberspace. On October 1, 2016, the United States officially handed over the management of Internet domain names to the non-profit organization Internet Corporation for Assigned Names and Numbers (ICANN), which nominally indicates the end of the era of unilateral monopoly on Internet core resources. But in fact, The US government can still arbitrarily control the ICANN's management rights, indirectly grasp the distribution rights of domain names and addresses, and monopolize the power of distribution of network resources. At the same time, the United States basically dominates every key link in the Internet industry chain, thereby enabling the large-scale monitoring of intelligence work and the hegemonic situation of information asymmetry by virtue of the advantages of Internet resource allocation and key aspects of the industry chain. Therefore, under the superiority of technical resources, the United States has realized the extension

[35] Robert Cox (1981), *Social Forces, States, and World Orders: Beyond International Relations Theory*, Millennium, Vol.10, No.2, p.126-155.
[36] Adam Segal (2016), *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Public Affairs, p.31.

and penetration of cyberspace from the economic, military and ideological levels. In the end, the United States has monopolized technical resources to promote information hegemony in cyberspace. As a power tool for US hegemonic protection, cyberspace presents a blueprint for the United States' "right to make Internet."

5.1.2. Construction of American cybersecurity discourse hegemony

Foucault's theory of discourse power pointed out that discourse is manipulated by power, which is a discourse constructed by power, and discourse in turn constructs power. The whole society is formed by the mutual construction of power and discourse. The advent of the cyber age has brought hope to people. In the cyber world, everyone is virtual. It provides a platform for people to show themselves. Everyone can freely communicate through the Internet. But the reality is that the cyber era has not escaped the manipulation of power. People express themselves in imaginary freedom. Foucault's theory of discourse rights also applies to the cyber age.

In the cyber space, we can also see the interaction between various forces. Because of the open, interactive, and shared nature of the Internet, people can interact freely through various discourse carriers (such as posts, pictures, videos, etc.). In the cyber space, every computer terminal is a node, which is a kind of power, which causes the power relationship in the Internet to always spread throughout the cyberspace in a state of “capillary”. Since the internet does not exist from the real society, the power relations in the cyberspace will also affect the entire human society in reality.

In addition, Foucault's theory of discourse power believes that power must be occult, while the object of power is visible, so that the discourse of the object of power can be effectively controlled. The emergence of the Internet makes this power technology more concealed, while the object of power More transparent, due to the anonymity of the network, people in today's society voluntarily express their true ideas on the Internet. Thus, the more they say, the stronger their power is, and the more they can control their discourse.

5.1.2.1. The concept and performance of American cyberspace discourse hegemony

"Discourse is power." Discourse and power are always in a relationship. In the view of the famous constructivist Alexander Winter, the national interest determines the specific behavior of the state, and deterinines the decision of the national interest is the concept, knowledge, identity, etc., he believed "Identity is the basis of interest"[37]. Therefore, different views on identity lead to the different pursuit of national interests. the United States' process of seeking online discourse hegemony is actually the process of shaping role identity. The discourse hegemony is a discourse system that is in a dominant position in the struggle against other discourse systems. It can transmit the ideas and cultures containing its own values and ideology to the audience through this dominant discourse, and it is continuously recognized by the audience. It reflects a relationship between hegemonic discourse and non-hegemonic discourse. Foucault believes that knowledge is hegemony, and it is also a kind of "discourse hegemony", which repeatedly emphasizes the hypocrisy of knowledge, which has become a tool for power to control others and protect their own interests. For a country's domestic politics, hegemonic discourse sometimes makes concessions and compromises to non-hegemonic discourse. For international politics, hegemonic discourse is more direct to the control and domination of non-hegemonic discourse. This is especially true for cyberspace where discourse is borderless, whoever has the discourse that can effectively influence others has the power to control others. Therefore, those who have power always try to construct discourse that can attract others' approval, and use the various media to transmit the discourses of cultural elements such as their own values to a wide audience around the world, thereby enhancing their power.

---

[37] Alexander Wendt (1992), *Anarchy is What States Make of it: The Construction of Power Politics*, International Organization, p. 46.

[37] The White House, "U.S International Strategy for Cyberspace: Prosperity, Security, and Open

5.1.2.2. Three aspects of the American cyber hegemony

First, control of cyberspace discourse. Since the birth of the Internet, the United States has seen the important role of the internet in spreading values and influencing national interests. Therefore, it has always sought the dominance of cyberspace discourse and influenced reality and international relations. At present, the United States accounts for 10 of the 13 domain name root servers in the world, including the main root server, and the other three are located in the United Kingdom, Japan and Sweden. Therefore, the United States theoretically has the ability to monitor and manage the network world. Under the new situation, the United States is using its dominant position in network technology and management to extend media discourse hegemony to the entire cyberspace and form a network discourse hegemony. In 2013, the “Snowden Incident” caused an uproar in the world, and the incident exposed the ambition of the United States to seek cyber hegemony. Among the contents revealed by former US Central Intelligence Agency (CIA) technical analyst Snowden, several US “prisms” were disclosed in secret surveillance projects. Snowden’s remarks have confirmed that over the years, the United States has owned the global internet infrastructure and core technologies. With these advantages, projects such as “prisms” have been carried out for governments, organizations, schools, enterprises, even individuals can conduct surveillance and cyber secret activities.

Second, English language priority in cyberspace. Although the internet is set up in multiple languages, the standard language is English, which is an exclusion for non-English speaking countries. In addition, today more than 100 countries around the world use English as a second language, which inevitably consolidates the language advantage of the United States in cyberspace.

Third, the control of cyber issues. The United States attaches great importance to the use of online media for topic shaping and discourse creation. It has compiled a series of discourse systems centered on the "Internet Freedom" system, and its right to interpret has always been in the hands of the United States. On the one hand, it can dilute the sovereign attributes of Internet management, facilitate its dissemination of American

values, and manipulate the trend of public opinion. On the other hand, it is also possible to legalize its interests.

5.1.3. Construction process of cyber discourse

In May 2011, the White House released the "U.S International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" report, which listed the seven policy priorities that the cyberspace is pushing forward[38]. Its content and objectives reveal the cyberspace scope extend to the global cyberspace. The construction process of US cybersecurity discourse hegemony includes: in the military field, the United States actively consolidates its cyber military hegemony status; at the international normative level, the United States adopts an international policy spillover form that constructs its own legitimacy and dissolves the legitimacy of others; at economic level, through technological and policy advantages, the United States preemptively expand their cyberspace alliance; in the ideology field, the United States forms a "internet freedom" camp, balancing the ideological discourse of China's cyberspace governance and cyberspace sovereignty .

The United States actively expands its cyberspace military hegemony. First of all, the US military level has shown a tendency to turn to the offensive. Among them, the most obvious signal of the militarization of the US internet is the establishment of the Cyber Warfare Command in the “U.S Cyberspace Policy Review” published in May 2009[39]. In March 2011, Keith Alexander, the commander of the US Cyber Command, outlined for the first time five strategic pillars to enhance the cyber warfare capabilities of the US military. In the same year, the US Department of Defense’s first Cyberspace Action Strategy officially promoted cyberspace the fifth field of military operations. Second, the US government reorganized and expanded the cyberspace. In March 2013, the Cyber Warfare Command added 40 new internet units; in March 2014, it explicitly proposed to invest in newly expanded cyber

[38] The White House, *U.S International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, https:// obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf

[39] U.S White House, *U.S Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communication Infrastructure*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ intemational_strategy_for_cyberspace.pdf

capabilities and build 133 network mission units. The cost of cyberattacks in the United States is 3-4 times higher than that in defense.

The United States constructs discourse hegemony through international policy spillovers. On the one hand, the United States took the lead in becoming the proponent and interpreter of cyber technology, and finally formed the policy barriers to cyber security by dissolving the legitimacy. Swedish scholar Iohan Eriksson once commented that "the perception of information security in most Western countries is actually influenced by American security perceptions[40]". The United States tried to grasp the right of interpretation and control in the field of communication by means of the Technical Standards Flow Chart. At the same time, the Global Internet Freedom Act promulgated in 2006, the International Strategy for Cyberspace in 2011, and the Tallinn Manual in 2013 is intended to emphasize that existing international legal rules apply to cyberspace. On the other hand, the United States regards countries that are actively involved in improving cybersecurity legislation as others. January 21, 2009 President Obama signed the Memorandum of Transparency and Openness, aimed at reaching a consensus on the interests of hegemonic powers. In the cyberspace conference held in London in 2011 and the Internet Freedom Conference in The Hague, US Vice President Biden and former Secretary of State Hillary Clinton publicly responded to other countries' doubts about cyber technology standards.

The United States has formed its own cybersecurity alliance strategy in various forms, broadly divided into the strategy of consolidating intimate alliances and striving for potential allies. First, the United States has consolidated its intimate alliances through issues such as cybersecurity incidents and cybersecurity exercises on the grounds of reducing cyberspace vulnerability. As a core member of NATO, the United States has spilled its own network security thinking into NATO. In the face of the cyberattack launched by international hackers against Estonia in 2007, the United States chose to lead NATO's key development network strategy. In May 2008, the NATO cooperative cyber defense excellence center was established in Tallinn. In addition, the US Department of Homeland

[40] Jphan Eriksson, *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, Routledge,2001, p.146.

Security has proposed a series of exercises such as cyber storm since 2006. The 1-2 year exercise focused on simulating cyber crises for key industries and improving large-scale cyber attacks affecting critical US infrastructure.

5.2. China’s cyberspace institutional discourse power

5.2.1. SWOT analysis of China's participation in global cyberspace governance

5.2.1.1. Advantages

China is a big Internet country with a certain scale advantage. According to statistics from Internet Live Stats, China is the country with the largest number of Internet users, accounting for 22% of the total number of Internet users worldwide. The overall level of China's Internet scale has increased rapidly, which also shows that China is trying to participate in global cyberspace governance and promote the transformation of the existing cyber system has gradually improved.

5.2.1.2. Disadvantages

First, China's participation in global Internet governance is relatively late and has not taken the lead. Although China's Internet technology has developed rapidly in recent years, China's access to global Internet services is late, and it is difficult to try to participate in the design of Internet rules and construct a new cyber order. At the same time, cyberspace and cybersecurity also reflect differences and conflicts among national ideologies and values. Western values still have an overwhelming advantage in today's cyberspace. This makes it difficult for China to catch up and overtake in this field.

Second, China's global cyber governance key technologies are insufficient in its own capabilities, and Internet resources are scarce. The urgency of the transformation from

“Made in China” to “China's Smart Manufacturing” is reflected in all aspects. The independent research and development capability of cyber technology is also a constraint factor for China's participation in global cyberspace governance. On some key technical issues, China's scientific research and development still rely heavily on foreign technology. In addition, in terms of Internet resources, one of the necessary infrastructures of the Internet, "Root Domain Name Server", currently has 12 top-level geographic domain name main servers in the world, belonging to three US companies, three US government agencies, two American universities, an American non-profit organization, a Swedish Internet exchange, a European network resource coordination center, and a Japanese agency. At present, compared with the Internet powers such as the United States, this is a problem that China needs to solve as a “cyberspace power”.

5.2.1.3. Opportunities

In fact, China's participation in global Internet governance and the process of building a community destiny of cyberspace is also a process of constantly remedying and overcoming its own disadvantages.

First, the unilateral control that the global cyberspace governance should not be subject to one big power has become a global consensus. Promoting the construction of a new global cyberspace governance order is the unanimous appeal of most countries. The statelessness of cyberspace determines that global cyberspace governance requires the cooperation of all countries. At the UN level, the World Summit on the Information Society (WSIS) has reached a common understanding of the digital divide and the cyber security, cyberspace governance, and cyber human rights in developing and developed countries. The 2016 G20 Summit in Hangzhou passed the “G20 Digital Economy Development and Cooperation Initiative” and reached consensus on the extensive cooperation among countries in the cyber field. It shows that most countries in the world recognize the necessity of cooperating and promoting the global cyberspace governance process. The benign interaction between countries has created a favorable background for China to expand its cyberspace strategic space.

Second, the US government has officially handed over Internet domain name management rights to ICANN (The Internet Corporation for Assigned Names and Numbers), which has driven the transformation of the global cyberspace governance landscape to a certain extent. The United States "transfer" Internet domain name management rights is essentially a strategic consideration for maintaining its cyber hegemony status. But in any case, the behavior itself releases a signal of the construction of a new cyberspace order and new rules.

5.2.1.4. Threats

First, China's participation in the external threat of global Internet governance has triggered the vigilance and suspicion of Western countries represented by the United States. At this stage, the United States remains the only superpower in the world. Sino-US relations are the most important bilateral relations in the 21st century. The rapid rise of China and the relative recession since the subprime mortgage crisis in the United States have further strengthened the possibility of "transfer of power" in the United States. In this context, China's participation in global cyberspace governance is bound to face various barriers built by the United States.

Second, other countries are also actively participating in the Internet competition and competing with China. As the “fifth space” outside the land, sea and sky, cyberspace has become a strategic competition for fierce competition in the world. In addition to the United States' desire to maintain its Internet dominance, other countries also hope that global Internet governance order and rules can be developed in a direction that benefits their national interests. In general, in terms of the construction of a new global cyberspace governance order, there are two main views: one is the “multi-stakeholder” model, and the other is the “multilateral government operation” model. The former advocates that in addition to the government, private institutions, public institutions, civil society, should share the right to Internet governance with the government. While the second view believes that within the UN framework, governments are global cyberspace governance dominates and emphasizes the important role of national sovereignty. At the 4th World Internet

Conference, president Xi Jinping expounded the concept of “internet sovereignty” and further reaffirmed the “multi-government operation” model advocated by China. However, some countries have the opposite attitude with China in this view. Taking the negotiation of the “WSIS+10” outcome document as an example, the United States, Germany, and BRICS countries including India and Brazil all support the “multi-stakeholder” program. It can be seen that even if the strategic objectives are the same or similar, there are not many opinions with China.

5.2.2. China's path to construct an institutional cyberspace discourse

5.2.2.1. Nationalism

The level of national governance is largely determined by the amount of power that can be obtained. The success of a country's domestic policy is directly related to the extent to which it is recognized by other countries and the international community. In an anarchic international society, sovereign states have the highest sovereignty within the country and the decision-making power of foreign autonomy. They are the primary subject of the construction of the discourse-type, transformational, and declarative institutional discourse power and the country that relies on the institutional discourse power. The path of doctrine is mainly reflected by the spillover effect of state governance, including: the spillover effect of economic growth in a country, the spillover effect of institutional reform, and the spillover effect of internal and external policy docking. The innovation of economic growth mode is the source of the establishment of institutional discourse power. Whether it is old capitalist countries such as Britain and the United States, or emerging developed countries such as Japan and South Korea, their growth patterns have undergone a transition from “labor-driven”, “capital-driven” to “management-driven” and “knowledge-driven”. Historical experience has shown that the shorter the time for the growth mode to change from extensive to intensive, the stronger the institutional innovation capability, and the stronger its ability to interface with the outside world.

5.2.2.2. Transnationalism

The ability to participate in transnational institutionalisms, as well as leadership, decision-making and contribution in these institutionalisms, are important indicators of the extent to which a country has and to what extent it has an institutional voice. Transnational institutionalism is a cross-domain platform for the construction of principled, normative, regular and procedural institutional discourse rights. The transnationalist path of institutional discourse power is mainly through various formal and informal interregional organizations and regional organizations. The international institutionalisms at the global level are embodied in the mobilization and coordination capabilities of sovereign states on transnational issues, the ability to interpret and apply international organization rules, and the leadership, organization and aggregation capabilities in regional affairs.

Unlike other paths, the transnationalist path seeks institutional discourse power in a collective form, specifically in two ways: the first is a cross-country cooperation institutionalism. The transnational cooperation institutionalism is an international cooperation institutionalism formed by international actors from different regions based on common identity, common goals and common interests. Although these institutionalisms do not reach the global scale in terms of participation and representation, their impact on world development is still extensive and far-reaching. For example, the Organisation for Economic Co-operation and Development (OECD) composed of 35 market economies, has greatly enhanced the discourse of member states in global economic, social and government governance. The BRICS composed by Brazil, Russia, India, China, and South Africa has rapidly increased the voice of the emerging market countries with promising prospects in participating in global economic governance. The second is the regional cooperation institution. The regional cooperation institution is a cooperative institution formed by international actors from the same region based on geographical proximity and common development needs. These institutionalisms are based on regionalism and intergovernmentalism, and fully embody the institutional discourse rights. For example, after the Second World War, the EU regained its institutional discourse in the form of a

super-national unity of European countries, playing an important role in reviving the European economy and consolidating the international status of European countries. ASEAN gained institutional discourse through independent and joint efforts of Southeast Asian countries which won a place for Southeast Asian countries discourse in the international relations.

5.2.2.3. Globalism

Institutional discourse power has the characteristics of intersubjectivity, and it needs to be based on international space. The status, image and prestige of a country in various global multilateral situations are directly related to the size of its institutional discourse power. The global mechanism is the broadest platform for the construction of principled, normative, regular and procedural institutional discourses. The globalist path of institutional discourse power is achieved within a global institutional framework in which the state provides global public goods to the international community through participation in global international organizations, global dialogue institutionalisms, and global multilateral diplomacy. This specifically shows as the ability of sovereign states to participate in global rulemaking, the ability to provide solutions to global problems.

The competition of world discourse is largely a dispute over the right to make international rules. Its core is the ability and willingness to provide the world with global public goods. At the background of insufficient institutional dynamics of globalization, China has gradually integrated into the tide of world development and deeply participated in the global institutionalism. The actions China took shows its ambition of building a new world system. In terms of philosophy, China proposes to build a new concept of "community of human destiny", upgrades its own development concept into global governance; incorporates the right of development into the vision of human rights, and proposes "development of the contribution to the enjoyment of all human rights" trying to redefine human connotations to break the Western monopoly on human rights discourse. In practice, China makes full use of the opportunities of home diplomacy and summit diplomacy, constructs a rich and diverse global consultation institutionalism, and strives to provide a “China program” for

the resolution of global problems. In 2014-2016, the World Internet Conference was held in Wuzhen, China for three consecutive years that shows China has actively established an international platform for interconnection with the world. In cyberspace governance, China proposed “Nine Initiatives”, “Four Principles”, “Five Proposals,” and “Four Goals” to build China’s discourse into a worldwide consensus. In April 2016, Xi Jinping proposed the “Four Proposals” to strengthen the international nuclear safety system at the 4th Nuclear Security Summit. He took the agenda and wrote it as a consensus conclusion in the 2016 Nuclear Security Summit Bulletin. The G20 Hangzhou Summit in September 2016 achieved three landmark “institutional innovations” in the summit to make progress in promoting the development-oriented issues and improving the global governance structure under the G20 framework. From the bilateral to the multilateral, from the consensus to the institutionalism, the “China Program” and the “China Concept” are at the global level.

5.3. The cyberspace game between China and the US

The development of cyberspace rules that both China and the United States can recognize and effectively put into practice is an important issue in current Sino-US relations. Cyberspace requires effective principles, norms, rules, and decision-making procedures to constrain it, which has become the consensus of both China and the United States. However, the Chinese and US governments still have a long way to go in terms of the content of cyberspace rules and the principles to be followed in building cyberspace rules. In terms of specific content, how to realize the coordination between the key resources of the network, the key technologies, the flow of information and the national economic, political and military security and the interaction between the United States and China are in a game. On the one hand, China and the United States need to form the consensus Institutionalization and effective implementation in practice. On the other hand, for areas that do not form a consensus and are closely related to each other's national interests, it is easy and difficult to promote the formation of cooperation in terms of fundamental principles and positions. China and the United States launched a deep game around the structure, function and culture of the cyberspace rules. Based on the interactive process

of China-US cyberspace rules, this part analyzes the competition and cooperation intervals, strategies and influencing factors of Sino-US games, and proposes a feasible path to promote Sino-US cooperation through institutional equilibrium.

5.3.1. The Sino-US game framework for cyberspace rulemaking

Game is the collective action of decision-making party seeking optimal decision-making coordination in the context of the coexistence of interest and conflicts. The Nash Equilibrium game is the most common type of game, which refers to the game process in which all decision-making parties seek the optimal combination of decisions. In Nash equilibrium, a single decision-making party does not realize the maximization of benefits, but a suboptimal strategy choice that must be made for it. All decision-making parties do not achieve the overall benefit maximization, but the decision-making parties make the best combination of decisions that can be made under certain conditions. The game between China and the United States around the development of cyberspace rules is a coordinated game for finding Nash equilibrium under incomplete information conditions.

5.3.1.1. Sino-US cyberspace game basic elements

The complete game contains five aspects: game subject, game information, strategy set, game order and game income[41]. In the game between China and the United States on the development of international rules for cyberspace, the following basic elements are included.

First, the subject of the game. The participants of the game are the Chinese and US governments and the relevant non-government actors in both countries. Both countries attach great importance to the formulation of cyberspace rules. China's advocacy of sharing key resources and core technologies in cyberspace which can bring benefits to all

[41] Pierre Allan, Cedric Dupont (1999), *International Relations Theory and Game Theory: Baroque Modeling Choice and Empirical Robustness*, International Political Science Review, Vol.20, No.1, p.23-47.

countries in the world, especially to developing countries, including promoting economic and social development and enhancing national security. This matches China's building a new world system to get rid of America's technical barrier. The United States hopes to rely on its advantages in key resources and core technology control to maintain its cyber hegemony. China advocates the principle of multilateralism and the United States adheres to the principle of multilateral stakeholders. At present, the United States has a leading advantage and is in a strong position in the formulation of international rules for cyberspace. China advocates that national codes of conduct, international law and trust measures related to international rules of cyberspace can correctly reflect the interests of developing countries. China and the United States use national interests as the basis for strategic choice.

Second, game information. The game between China and the United States around the cyberspace rules is an incomplete information game, but China and the United States will communicate at various levels, such as the meeting between the heads of China and the United States, the China-US Strategic and Economic Dialogue, the joint fight against cybercrime between China and the United States, high-level expert group meeting of China-US cyberspace international rules and other institutionalisms to express their own interests and core concerns. China and the United States are also completely rational actors, in order to maximize their national interests, China and the United States will conduct an infinite number of repeated games around the formulation of cyberspace rules.

Third, the set of strategies for the game subject. From the perspective of game theory, China and the United States have the following four strategic combination hypotheses in the formulation of cyberspace rules: (1) China and the United States have chosen a strategic combination of cooperation, indicating that both China and the United States agree on the importance of formulating effective cyberspace rules and urgency. The United States has a tolerant attitude toward China's position and principles, although there are the applicability of the United States to cyberspace sovereignty, the importance of sovereign governments in the jurisdiction of the network, and the transfer of cyberspace international rules, conservative positions in key areas of cyberspace and sharing of core technologies,

the United States is willing to negotiate on the above issues. China is willing to recognize the US's first-mover advantage in key cyber resources and cyber technology control, and the multi-stakeholder model. It is reasonable to absorb and is willing to cooperate with the United States to promote the consultation process of cyberspace rulemaking on the basis of maintaining and realizing national interests and promoting the development of global cyberspace equity and justice. (2) The combination of China's choice of cooperation and the United States' choice of non-cooperation means that the United States does not agree with the core position of the government advocated by China in cyberspace governance, and is unwilling to use the UN framework to promote the process of cyberspace international rulemaking and adhere to multilateral interests. It chooses to hold the principle of unwilling to share the dominance of global cyberspace governance with other countries. (3) China's choice of non-cooperation and the United States' choice of cooperation strategy, indicating that China denies the US's current multi-stakeholder principle. It chooses to unite other forces of the international community and reinvigorates the country's cyber resources and technology control and possession to promote the United States to accept China-led international institutionalisms for global cyberspace governance. (4) Both China and the United States have chosen a combination of strategies that do not cooperate, indicating that China and the United States compete comprehensively in the development of key resources and c core technologies in cyberspace, and strive to have comparative advantages. Both China and the United States deny each other the basic principles for the formulation of international rules for cyberspace. The position that the principle of multilateralism and the principle of multilateral stakeholders are fundamentally opposed, and the realization of the other principles and opinions is the threat and damage to the national security of the country. Both China and the United States are committed to gaining dominance in the governance of global cyberspace, meanwhile to curb the efforts of the other side to promote the realization of their national interests.

5.3.1.2. Influencing factors of Sino-US game in the development of cyberspace rules

Under the current international situation and the changing environment of Sino-US relations, based on the consideration of the overall national interests, the game between China and the United States in cyberspace governance will not be a complete cooperative game, that is, not all fields will be governed in cyberspace. It will not be a complete non-cooperative game, because the cost of the complete confrontation between the two sides will outweigh the benefits. The game attribute of China and the United States in cyberspace is a coordinated game, that is, both competition and cooperation coexist, and the interval between competition and cooperation lies between full cooperation and complete non-cooperation.

In terms of the necessity and importance of building international rules for cyberspace, China and the United States have consensus and formed cooperation in the following aspects. First, China and the United States hope to maintain and build the peace, security and stability of cyberspace with international rules. They agree with the principle that information and communication technology should be applied to peaceful purposes, established by the United Nations Information Security Government Expert Group meeting.. Second, global cyberspace is not an extraterritorial place. China and the United States believe that international rules bring national sovereignty to the maintenance of information and data security, as well as to preventing, combating and containing cyber warfare, economic espionage, cybercrime and cyber terrorism. The threat of security and development benefits is critical. Third, China and the United States agree that the relevant principles and spirits represented by international law, especially the United Nations Charter, represented by the principle of national sovereignty apply to cyberspace. This consensus was respectively reported in the report of the 2013 and 2015 United Nations Information Security Government Expert Group Meeting[42].

[42] United Nation, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Jun. 26, 2015, https :/

There are different levels of disagreement between China and the United States on the principles to be followed in the construction of international rules for cyberspace and the rules governing the key resources, core technologies, and state behaviors in cyberspace. The attribute problem of the cyberspace, in which the issue of cyber sovereignty is the core of the attribute problem. How to understand and grasp the principle of cyber sovereignty and how much jurisdiction the sovereign government has in the domestic and international governance of cyberspace is the Sino-US root cause of the divergence. The United States believes that cyberspace has the global public domain nature. The dissemination of internet information, the application of technology and the activities of personnel in cyberspace are superior to government jurisdiction. The information dissemination and information activities related to networks should be made by individuals, NGOs, and professionals. The jurisdiction of the community, enterprises and other actors, the government's jurisdiction should be limited. China believes that the attribute of cyber sovereignty is the essential attribute of cyberspace. The cyber frontier is a natural extension of national sovereignty. The cyberspace activities within it have the highest jurisdiction, and adherence to the principle of respect for cyber sovereignty is the key to advancing the transformation of the global cyberspace governance system. Respect for the principle of cyber sovereignty is the fundamental starting point of the Chinese program. Significantly different from China's position on cyber sovereignty, although the United States recognizes that sovereign governments have jurisdiction over cyberspace activities within sovereignty, it clearly states that such jurisdiction is limited. The reason is that sovereign governments jurisdiction must be consistent with applicable international law, including international human rights obligations. The government cannot invoke the concept of national sovereignty to over-regulate cyberspace activities on the grounds of counter-terrorism and anti-extremist violence, such as reviewing cyber content or restricting access to the internet[43]. In 2010, Google's withdrawal from China' was a typical manifestation of the differences between China and the United States on the issue of cyber

/digitalwatch.giplatform.org/processes/ungge.

[43] Brian J. Egar:"International Law and Stability in Cyberspace",Berkeley Journal of International Law, Vol.35, No.5, 2017, pp.169-180.

sovereignty. In this incident, the United States and other Western countries adopted the provisions on freedom of expression in international human rights law and the trade in goods in the WTO law.

Second, the platform of cyberspace governance. At present, the international community lacks a platform that can better coordinate the interests of all parties, has broad representation and can lead the formulation of international cyberspace rules. Around the formulation of cyberspace rules, the international community has divided into a representative of the developed countries of the United States and Europe and emerging powers represented by China and Russia. China advocates the United Nations as the main platform for cyberspace governance, and fully utilizes the role of institutions such as the International Telecommunication Union to promote the development of international rules for cyberspace that are generally accepted by all parties. Thus, cyberspace governance can be widely represented and produced whose results can benefit the developing countries more. Correspondingly, although the United States supports the active role of the United Nations in the cyberspace rulemaking process, it has undoubtedly has more institutional platforms and policy options for cyberspace rulemaking than for emerging developing countries. For example, although the Tallinn Manual comes from the US-European knowledge community, the United States and its NATO allies can use this manual to seize the dominant position in the formulation of cyber war rules.

In conclusion, cyberspace governance is one of the most controversial issues in Sino-US relations. From a macro perspective, China and the United States have not yet reached a comprehensive consensus on the rights, obligations, standards of conduct, and international norms of sovereign states in the cyberspace. Because as two main actors, China and the United States have a decisive influence on the international system and the international order. China-US differences in ideas and interests in cyberspace governance will have a negative impact on Sino-US bilateral relations, peace, stability in the Asia-Pacific region, and global political order. The Chinese side believes that the global cyberspace lacks comprehensive traffic rules, and it is of vital importance to establish international consensus and international norms. China and the United States should work

together to help build the basic order and rules of cyberspace, and propose the basic principles of establishing network behavior based on the UN framework. The formal, continuous, and substantive Sino-US consultation institution is extremely necessary to reduce the uncertainty in Sino-US bilateral relations and the behavior of countries that are detrimental to bilateral relations.

5.3.2. Game focus of Sino-US cyberspace

With the advancement of science and technology, the popularity of information has become higher and higher, the world has entered the era of big data, and the application of cyberspace has already entered various fields of the world. With the multi-dimensionality of cyberspace applications, cyberspace technology and its various industrial chains have become one of the most important focuses of countries in online competition.

China and the United States have principled differences in the construction of the cyberspace governance system. This principled disagreement is structurally different and difficult to reconcile. Faced with the same demands of the two countries on the dominance of the Internet, China and the United States are particularly fierce in the choice of freedom of speech and governance in cyberspace. The core principle of the US cyberspace governance system is "to adhere to the free mobility of information," which is an inevitable continuation of the "Internet openness" in the United States. It means that the United States insists that the free flow of information is the universal "human rights freedom" that the United States wants to universalize. The US insists that the free flow of information is an important basis for the progress of human society. It has also advocated that the international community should fully open the Internet and let information flow freely without restrictions or obstacles. Since the US government believes that international human rights principles are universal that must apply to cyberspace, and there is no need to set rules and restrictions on the free flow of information. This is the contradiction of freedom of information in the United States and the information regulation being implemented in China.

Finally, due to different governance principles, China and the United States have chosen different governance models. The West headed by the United States believes that the future cyberspace should be based on the different core functions of the Internet to develop a corresponding free order. The core functions of the Internet are mainly divided into three parts: content, source code and physical technology layer. The West believes that the governance of source code and physical technology layers should be placed in a “multi-stakeholder” model, while the governance of online content is more related to political content.

Compared with China, under the government's leadership the “government-led model” conducts information screening and centralized supervision on the domestic internet, and there are corresponding laws that restrict the information content and flow form under the government-led framework. In recent years, hackers and some unscrupulous groups have committed madness in cyberspace for different interests. In addition, terrorism has spread to the Internet. Governments have introduced corresponding legal policies to strengthen the overall supervision of cybersecurity. China was not immune to this storm but the impact can be minimal. It can be seen that the government regulates the virtual space of the network by enacting laws. On the one hand, it can ensure the legality of the private economic groups and the society that use the network to operate, and on the other hand, it can ensure that its rights and interests are not invaded by cyber attacks. At this point, it has advantage than the “multi-stakeholder” governance model.

6. Conclusion

The overall game between China and the United States in cyberspace is caused by the different political concepts and cultures of China and the United States. In recent years, China has increasingly advocated the "sovereignization" of cyberspace, while the United States insists on cyberspace freedom, the conflict between the two has led to competition in other fields. The most important focus of international attention is the game between the two sides in building future cyber rules, game for cyber security governance, and military

game at the cyberspace level. On the whole, the competition between China and the United States in cyberspace has the following three characteristics:

First, the discourse competition trend between China and the United States is obvious. At this stage, cyberspace has penetrated into various fields of the country and played an increasingly important role. Therefore, the development of cyberspace security has already risen to the national security system and has become an important part of building a national security strategy. The trend of competition between China and the United States in cyberspace is in positive contrast with the strength of China and the United States. It is a comprehensive realization of the two countries' dominance of the future world cyberspace rules and the competition for cyberspace governance rights.

Second, the structural contradictions between China and the United States in cyberspace competition are obvious. The reason why the competition between China and the United States in cyberspace has become more and more fierce is rooted in the differences in the political system, national conditions, national culture and values of the two countries. It is precisely because the world hegemony of the United States' judgement of the rise of the Chinese powers and led to the deployment of the United States. The awareness created a series of strategies for China, such as “Strategy for Cyberspace”. The militarization of cyberspace initiated by the United States in order to maintain its status as a cyber hegemon also reflects the determination of the United States to maintain absolute freedom of cyberspace and to uphold the openness of cyberspace portals. This is structurally related to the “sovereigntization of cyberspace” advocated by China. The contradiction, the irreconcilability of this contradiction, has in turn promoted the fierce competition between the two countries in cyberspace.

Third, China and the United States have demonstrated cooperation opportunities in the cyberspace competition. Although China and the United States continue to compete in the field of cyberspace, cyberspace has the basic attributes of "international public domain". Therefore, the competition between China and the United States in cyberspace has triggered a series of vicious incidents. The violent hacking incident and the planning of the network black production are the best examples. In this case, for their own interests and

the stability of the world cyberspace, the two countries started active dialogue and cooperation, from the emergence of the China-US cyberspace forum to the successful multinational law enforcement, which demonstrates the great prospects for cooperation between the two countries in cyberspace.

7. Bibliography

Joseph S. Nye, Bookshelf, *The Power of Information*, Wall Street Journal, 10 September 1992.

Andrei Krutskikh, Galina Kramarenko (2003), *Diplomacy and the Information Revolution*, International Affairs, Vol 49, No. 5, p. 116.

David J. Rothkopf (1998), *Cyberpolitik: The Changing Nature of Power in the Information Age, Journal of International Affairs*, Vol 51, No. 2, p. 345.

[1] Xiao Zong, 《信息安全与信息战》, Tsinghua University, 2003, p. 7-8.

[1] Johan Eriksson, Giampiero Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)Relevant Theory?*, International Political Science Review, Vol 27, No. 3, p. 221—244.

[1] Johan Eriksson, Giampiero Giacomello (2006), *The Information Revolution, Security, and International Relations: (IR)Relevant Theory?*, International Political Science Review, Vol 27, No. 3, p. 227.

[1] Ole Wæver (2011), *Politics, Security, Theory*, Security Dialogue, Vol 42, No. 4–5, p. 465–480. https://doi.org/10.1177/0967010611418718

[1] Yuan Sha (2017), *Discourse Checks and Balances Hegemonic Protection*, World Economics and Politics, No. 3, p. 85-107.

[1] Shen Yi (2014), *Global Cyberspace Governance and BRICS Cooperation*, International Watch, No. 4, p. 145-157.

[1] Michel Foucault (1994), *The Order of Things*, Reissue.

[1] Michel Foucault(1969), *The Archaeology of Knowledge,* Random House USA Inc, New York, United States.

[1] Michel Foucault (1999), *Society Must Be Defended*. Abnormal, p 23-26.

[1] Steven Best, Douglas Kellner(1997), *Postmodern Theory*, The Postmodern Turn.

[1] Michel Foucault (1989), *Foucault Live: Interview*, Semiotext New York, p. 210.

[1] Michel Foucault, The Archaeology of Knowledge, Gallimard; GALLIMARD edition (February 7, 2008)

[1] Wu Zhicheng, Dong Zhuangzhuang (2016), *International System Transformation and China's Response*, Contemporary World, No. 5, p. 11

[1] Andreas Hasenclever, Peter Mayerand Volker Rittberger (1997), *Theories of International Regimes*, London: Cambridge University Press, p. 1-2.

[1] Robert Crawford (1996), *Regime Theory in the Post-Cold War World: Rethingking Neoliberal Approaches to International Relations*, Dartmouth: Darmouth Publishing Company, p. 57.

[1] Stephen Krasner (1985), Structural Conflict: *The Third World Against Global Liberalism*, Berkelay: University of California Press, p. 7-9.

[1] Andrew Kydd and Duncan Snidal (1993), *Progress in Game-Theoritical Analysis of International Regimes, in Volker Rittberger (ed.)*, Regime Theory and International Relations, Oxford: Clarendon Press, p. 112.

[1] Kenneth Neal Waltz, Waveland Press; 1 edition (February 5, 2010), p. 150

[1] Joseph S. Nye, Jr. (1999), *Redefining NATO Mission in the Information Age*, NATO Review, Vol 47, No. 4, p. 12.

[1] John Naisbitt, *Megatrends Asia: the Eight Asian Megatrends that are Changing the World*, Nicholas Brealey, 1995.

[1] Robert O. Keohane, Joseph S. Nye Jr. (1998), *Tower and Interdependence in the Information Age*, Foreign fairs, Vol 77, No. 5, p.84.

[1] PCCIP: *President's Commission on Critical Infrastructure Protection.* At http://www.info-sec.com/pccip/web/backgrd.html. (accessed on 20/06/2002)

[1] Xiaozong (2003), *Information Security and Information Warfare*, Tsinghua University Press, p. 12.

[1] *The "Future of Warfare"*, Economist, 8 March 1997. at http: www.economist.com/tfs/archive-trameset.html. (accessed on 11/01/2009).

[1] David J. Rothkopf (1998), *Cyberpolitik: The Changing Nature of Power in the Information Age*, Journal of International Ajfairs, Vol 51, No. 2, p. 344.

[1] Yuan Sha, *The Balance of Discourse and Hegemony Protection, World Economics and Politics*, No. 3, 2017, p. 85-107.

[1] Arnold Wolfers (1962), *Collective Defence Versus Collective Security,* The Johns Hopkins Press, p.183.

[1] U.S Department of Defense, *The Department of Defense Cyber Strategy*, https://www.defense.gov/Portals/1/features/2015/0415_ cyber-strategy/Final_2015—DoD_CYBER—STRATEGY—for—web.pdf

[1] Ferdinand de Saussure, Perry Meisel, Haun Saussy, Wade Baskin (2011), *Course in General Linguistics*, New York:Columbia University Press, p.20.

[1] Joseph S. Nye, Robert O. Keohane (2011), *Power & Interdependence,* Pearson, 4

edition, p. 40-44

[1] Steven Weber, Bruce Jentleson, The End of Arrogance: America in the Global Competition of Idea, Cambridge: Harvard University Press, 2009, pp.148-160.

[1] Robert Cox (1981), *Social Forces, States, and World Orders: Beyond International Relations Theory*, Millennium, Vol.10, No.2, p.126-155.

[1] Adam Segal (2016), *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Public Affairs, p.31.

[1] Alexander Wendt (1992), *Anarchy is What States Make of it: The Construction of Power Politics*, International Organization, p. 46.

[1] The White House, "U.S International Strategy for Cyberspace: Prosperity, Security, and Open

[1] The White House, *U.S International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, https:// obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_ strategy_for_cyberspace.pdf

[1] U.S White House, *U.S Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communication Infrastructure*, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ intemational_strategy_for_cyberspace.pdf

[1] Jphan Eriksson, *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, Routledge,2001, p.146.

[1] Pierre Allan, Cedric Dupont (1999), *International Relations Theory and Game Theory: Baroque Modeling Choice and Empirical Robustness*, International Political Science Review, Vol.20, No.1, p.23-47.

[1] United Nation, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Jun. 26, 2015, https :/ /digitalwatch.giplatform.org/processes/ungge.

[1] Brian J. Egar:"International Law and Stability in Cyberspace",Berkeley Journal of International Law, Vol.35, No.5, 2017, pp.169-180.