



## **The Competition between Sino-US Cyber Security since the Administration of Barack Obama**



**Siqi Zheng**

Supervisor: Professor Xue Wu, Professor Fuzuo Wu

Date of submission: May 2019

Keystrokes (general text, footnotes, and bibliography): 119,737

## CONTENT

1. Summary .....	2
2. Introduction .....	4
2.1 Research question .....	5
2.2 Literature review .....	6
3. Methodology .....	10
3.1 Research methods .....	10
3.2 Justification for theories .....	11
3.3 Justification for chosen data .....	11
3.4 Structure .....	12
3.5 Limitation .....	13
4. Theory .....	14
4.1 Interdependence theory .....	14
4.2 National interest theory .....	16
4.3 World system theory .....	18
5. Case analysis of Sino-US cyber security competition.....	21
5.1 Prism gate event.....	22
5.2 ZTE Huawei event .....	24
6. Political and economic analysis .....	27
6.1 Global network and new world economy .....	27
6.1.1 Changes in factors of production .....	27
6.1.2 Interdependence of the network and the new world economy .....	30
6.2 Cyber security and economic growth .....	32
6.2.1 Institutional environment.....	33
6.2.2 Technological innovation.....	34
6.2.3 Economic security .....	37
6.3 Sino-US cyber security under the evolution of the international system.....	40
6.3.1 Sino-US relations under global competition.....	41
6.3.2 Maintenance of the US hegemonic system.....	44
6.3.3 The rise of China in the world system.....	47
7. Conclusion .....	50
8. Bibliography.....	53

## **1. Summary**

In today's world, the information technology revolution is changing with each passing day. The network has penetrated into the international political, economic, military, and social fields, and has had a profound impact on its development. Globalization and informatization promote each other. The network has been integrated into all aspects of human social life, greatly changing people's production methods and lifestyles, and integrating countries around the world into an interdependent international system. At the same time, the issue of cyber security has become more important. On the issue of cyber security between China and the United States, there is both cooperative and competitive side. At present, combating cybercrime is the main area of cooperation on cyber security issues. In terms of domestic network security legislation, network security technology, network militarization and international cyberspace rules, the mutual competition is higher than the cooperation between the two countries. Especially since the Obama administration took office, after the prism gate event, the issue of Sino-US cyber security competition has become a prominent issue. For a better explanation, I attempt to analyze from the perspective of international political economy. Although there is no cyber security topic in the research topic of international political economy, but cyber security plays a very important role in shaping a new global market and in promoting economic growth. Undoubtedly, the network as a dominant production factor, its role in economic development has surpassed the production factors such as capital and labor, and has become a dominant production factor. As a production factor, the network's movement will inevitably have a corresponding impact on the international system, the relationship between the states, and the structure and political processes within the country. Therefore, international political economic analysis of cyber security issues is considered to be feasible.

China is a developing country, while the United States is the world's largest developed country. Both China and the United States face threats from each other or other countries in terms of cyber security, but the two countries have different security

strategies. The US cyber security is more "offensive", and China is still on the "defense". The control of network technology and the ability to deal with cyber security are both asymmetric. Faced with an asymmetrical national cyber security environment, China and the United States are eager to seize the dominant position in future economic development when dealing with the challenges of the big data era. This has led to the emergence of conflicts between China and the United States, and has to face the dilemma that has already fallen into the trap of developing a network security cooperation mechanism.

With the change of dominant production factors, cyber security plays an increasingly important role in economic development, which is related to technological innovation, economic security and the sound operation of the institutional environment. At the moment, the United States seeks to maintain its hegemonic status, while China is trying to rise in the dominant international system of the United States. Under the increasing mutual distrust and fierce competition that China and the United States have formed, the two countries will certainly make the necessary interests game in cyber security.

## **2. Introduction**

In recent years, with the popularization of the Internet and the continuous development and transformation of information technology, on the one hand, it has brought great changes to people's lifestyles, promoted communication between people, and strengthened exchanges between countries around the world. On the other hand, the development of computers, driven by commercial interests and political interests, has become a tool for individuals, enterprises, and even the country to seek economic and political interests, posing great threats to personal privacy, corporate interests, and even national security. From the US excuses that China's two major communication technology providers, ZTE and Huawei, have banned the national security of the United States, and the prism gate event has continued to ferment, cyber security competition has become one of the most important issues affecting Sino-US relations.

The theoretical significance of this thesis is to provide a new analytical perspective for Sino-US cyber security competition, which will help to understand cyber security comprehensively and deeply. There are different perspectives in analyzing the issue of cyber security in China and the United States. One is computer scholars and network professionals, they are more concerned with analyzing cyber security from the network technology level, providing technical support for network security and proposing technical solutions. One is international political scholars, they are based on international political theories such as realism and liberalism to explain the cyber security issues between China and the United States, and put forward some policy recommendations. There are also economists or economic observers who explain cyber security from the perspective of the relationship between cyber security and economic development and economic security. These explanations all have their rationality, show their multiple observational perspectives, and make the research of the problem deeper and more convincing. However, due to the complexity of cyber security, it is difficult to make a more detailed analysis of cyber security issues between China and the United States simply by considering a single angle and linear thinking. For example, when analyzing the problem of cyber security, only from a

single perspective, it will be difficult to understand the causes of cyber security, the feasibility of the measures taken and the reliability of the operational mechanism. It is also difficult to understand why the two countries have never been able to reach a consensus on cooperation on some issues related to cyber security.

This thesis analyzes the cyber security of China and the United States from the perspective of international political economics. Another theoretical significance is the innovative introduction of cyber security into the analytical framework of international political economy. International political economics mainly studies the impact of transnational flows of economic factors (including capital, technology, labor, and information) in the international system on the international system itself, state-to-state relationship, and the political structure and processes within the state.<sup>1</sup> In the past, the topics of international political economy were mostly concentrated on issues such as international trade, international finance, international investment, exchange rate, and national development. The emergence of cyber security issues is mainly due to the negative impact of the flow and diffusion of technological factors. The flow of network technology as a factor of production has had a very large impact on the international system, inter-state relations, and internal political structure of the country. Therefore, it is reasonable to introduce cyber security into the analytical framework and issues of international political economy.

## **2.1 Research question**

This thesis aims to answer the following research questions:

- 1) *Why cyber security has become an obstacle to the political and economic development of China and the United States? The emergence of such obstacles based on what level of consideration?*
- 2) *In the context of the new world economy, what changes have occurred in the relationship between China and the United States caused by cyber security?*

---

<sup>1</sup> Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010, p. 5.

## 2.2 Literature review

In China, the research on the Sino-US cyber security mainly includes the following points: 1. The process of promoting the implementation of cyber security strategy in the United States. 2. Competition and cooperation between China and the United States in the field of cyber security. 3. The multi-faceted impact of cyber security. 4. Cyber terrorism that threatens the network environment and even everyday life.

In terms of US national cyber security and information security strategy. In the book "National Cyber Security Strategy", author Shen Yi discussed the strategy adopted by the United States to ensure Internet security based on time changes, and proposed three processes of defense, control and shaping of the US cyber security strategy.<sup>2</sup> In his book "National Information Security Strategy of the United States ", Cai Cuihong gave a detailed definition of information security and security strategy at the beginning, analyzed the specific cyber security situation currently facing the United States, also proposed a strategy for the United States information security.<sup>3</sup> In addition, Cheng Qun also in his article "Analysis of the Obama Administration's Cyber Security Strategy", with his own unique perspectives and insights, made a profound analysis of the US cyber security strategy during the US President Barack Obama's administration, from the aspects of network security organization setting, personnel arrangement, and emergency response measures, it clearly shows the changes in the status of cyber security issues in different periods of Obama's administration. This will help us to further understand the US cyber security strategic plan during the Obama administration.<sup>4</sup>

In the competition and cooperation between China and the United States, Shen Yi in the article "Cognition, Competition and Cooperation in Digital Space —

---

<sup>2</sup> Shen Yi: "National Cyber Security Strategy", Beijing: Current Affairs Press, 2013, pp. 1-2

<sup>3</sup> Cai Cuihong: "National Information Security Strategy of the United States", Shanghai: Xuelin Press, 2009, pp2-4, pp72-109.

<sup>4</sup> Shen Yi: "Analysis of the Cyber Security Strategy of the Obama Administration, Modern International Relations", No. 1, 2010, p. 8.

Network Security Relationship under the Framework of Sino-US Strategic Relations", an in-depth analysis of the root causes of conflicts between China and the United States on cyber security. By means of Chinese hackers and freedom of information, the root causes of cyber security issues in the two countries are not in the network itself, but in structural contradictions among major powers, lacking strategic mutual trust, and emphasizing that correct governance measures should be managed in a relatively stable and acceptable level.<sup>5</sup> At the same time, he also focused on what is cyber security in the article "Network security and non-traditional factors in Sino-US security relations", and different from the traditional security factors, non-traditional security threats become new factors that can affect Sino-US bilateral relations.<sup>6</sup>

In terms of the impact of cyber security, Hu Jian and Wen Jun's joint article "Network and National Security" emphasizes the continuous development of Internet technology, interrupts the state's control over information, the government's fairness, social democratization, etc. The authority of the national government is also gradually changing. In this way, the stability of the government is reduced and politics is challenged as never before.<sup>7</sup> Wang Jinshui and others elaborated on the subtle relationship between online political participation and political stability in his article "On the Network Political Participation and Political Stability Mechanism". As for the topic of cyber terrorism, it has risen relatively early. At the beginning of the 21st century, there were many research results. For example, Tang Yan, Liu Qiang and Tian Jia published many articles on cyber terrorism during this period, and discussed cyber terrorism from various angles.

Western scholars have studied more about network deterrence, cyber warfare, and the development of international network governance rules.

In terms of network deterrence and cyber warfare, many scholars believe that there is uncertainty. Rid Thomas highlights the violent turmoil and uncertainty of cyber warfare in "More Attacks, Less Violence ". Unlike traditional warfare, cyber

---

<sup>5</sup> Shen Yi: "Cognition, Competition and Cooperation in Digital Space — Network Security Relationship under the Framework of Sino-US Strategic Relations", *Diplomatic Review*, No. 2, 2010, p. 38.

<sup>6</sup> Shen Yi: "Network Security and Non-traditional Factors in Sino-US Security Relations", *International Forum*, Vol. 12, No. 4, 2010, p. 59.

<sup>7</sup> Hu Jian, Wen Jun: "Network and National Security", Guiyang: Guizhou People's Publishing House, 2002, p.99.



warfare has an impact by means of disrupting the software system, and there is uncertainty as to whether the attack on the objective object can achieve the expected effect.<sup>8</sup> But in another article, "Cyber war will not take place," he emphasized that there is a big difference between cyber attacks and cyber warfare, and that the possibility of a cyber war is extremely low.<sup>9</sup>

In terms of cyberspace cooperation governance, the research of Western scholars has also begun earlier. In 2000, Gregory D. Grove and others emphasized in the "Cyber-attack and International Law" that cyber attacks are extremely harmful, seriously threatening national security, and directly pointed out that the current response measures are relatively negative, effective response measures should include the development of laws for transnational network operations and so on.<sup>10</sup> Tikk Eneke also gave the most important 10 principles to be followed in the international cooperation on cyber security between countries in his article "Ten Rules for Cyber Security".<sup>11</sup>

In addition, many scholars have done some research on the issue of Sino-US relations in the field of cyber security. Among them, the Brookings Institution scholars Peter W. Singer and Kenneth Lieberthal have jointly published "Cyber Security and U.S-China Relation". It focuses on the many problems that exist between China and the United States in cyber security cooperation, such as lack of strategic trust and differences in governance concepts. However, it was finally proposed that China and the United States only require to seek common ground while reserving differences, enhance the level of strategic mutual trust and strengthen bilateral communication, the limited cooperation between the two countries in the field of cyber security is entirely feasible.<sup>12</sup>

The literatures mentioned above all provide a useful contribution to the study of Sino-US cyber security. The downside is that the perspective of studying cyber

---

<sup>8</sup> Rid Thomas: "More Attacks, Less Violence", *Journal of Strategic Studies* 36, no. 1, 2013, pp.139-142.

<sup>9</sup> Rid Thomas: "Cyber war will not take place", *Journal of Strategic Studies* 35, no. 1, 2012, pp.5-32.

<sup>10</sup> Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik: "Cyber-attack and International Law", *Survival* no.3, 2000, pp89-103.

<sup>11</sup> Tikk Eneke: "Ten Rules for Cyber Security", *Survival* 53, no.3, 2011, pp.119-132.

<sup>12</sup> Peter W. Singer and Kenneth Lieberthal: "Cyber security and U.S-China Relation", 21<sup>st</sup> Center Defense Initiative at Brookings, Feb.2012, pp.31-33.

security in China and the United States is single and not comprehensive. Based on this, this thesis combines the research results of cyber security, Sino-US relations, international political economics theory, political and economic relations, etc., analyzes the cyber security issues of China and the United States from the perspective of international political economy, and provides some useful thoughts for the study of cyber security in China and the United States.

### **3. Methodology**

#### **3.1 Research methods**

The first research method is the case study method. As a common analysis method, select a case in a broader category and study an object whose meaning is beyond its boundaries. It is a method of actual description and theoretical analysis of an event with typical characteristics of the objective world. This thesis will select two typical cases with different perspectives from the Sino-US cyber security competition. From the national level, I chose the prism gate event. It is precisely after this incident that a crisis of trust has emerged between China and the United States, which has led to an increase in cyber security competition between the two countries, while cyber security cooperation has been slow. Through analysis, I will further explore the political and economic thinking brought about by China-US cyber security competition. From the enterprise level, I chose the event in which the two major communication service providers in China, ZTE Huawei, were investigated and blocked in the United States. The US's trade protectionism in the name of threatening its national security to suppress Chinese companies is an open challenge to the global free trade order. And behind this, it also triggered my thinking about the Sino-US cyber security game based on national interests.

Secondly, the comparative research method is chosen. The comparison is the most commonly used thinking method to understand the similarities and differences of things. Comparative research methods are now widely used in various fields of scientific research. In international political science research, comparative research is an important research method. The comparative research methods in this thesis include horizontal comparison and vertical comparison. The horizontal comparison includes China's cyber security policy and US cyber security policy, China's foreign policy toward the United States and US foreign policy toward China. The vertical comparison includes changes in Sino-US relations, changes in China-US cyber security policy, and changes in the strength of China and the United States within the

international system.

Thirdly, the deductive method is also very important in this thesis. By comparing these issues, further deducting China and the United States on these issues, to prove the feasibility and reliability of the analytical perspective.

### **3.2 Justification for theories**

In view of cyber security competition issues, from different perspectives, there are different interpretations. In this thesis, I attempt to use the three theories of international political economy, namely, interdependence theory, national interest theory, and world system theory. Although there is no cyber security topic in the research topic of international political economy, cyber security plays a very important role in shaping a new global market, and cyber security plays an important role in promoting economic growth. The network undoubtedly has a role in economic development as a dominant factor of production that exceeds the role of capital as a dominant factor of production. The flow and movement of the network as a factor of production will inevitably have a corresponding impact on the international system, the relationship between the states, and the structure and political processes within the country. And cyber security is the subject of ensuring the security of the network as a factor of production. Therefore, it is feasible to do international political economics analysis on cyber security issues. I will provide further justifications for my theory choice in the theory chapter.

### **3.3 Justification for chosen data**

In terms of data selection, I first looked at the official statements of China and the United States, most of which came from the White House and China Cyberspace Security Association, as well as reports and other first-hand information, such as the US National Security Strategy Report. Secondly, the political and academic circles of China and the United States also have a large number of bilateral dialogue

mechanisms and forum activities on the cyber security relationship between the two countries. In addition, I also use newspapers, websites and other news media resources, such as Xinhuanet. And obtain literature on Chinese and American journal full-text databases, China National Library, and thesis database retrieval. These all provide useful data for my thesis.

### **3.4 Structure**

This thesis is divided into 7 parts. The first summary part indicates that after the Obama administration took office, the issue of cyber security has become more prominent. The issue of global cyber security has been put on the agenda of various countries and is regarded as part of the national security strategy. Cyber security competition has also become an issue that is urgently awaiting resolution of the development of Sino-US relations. The second introduction part mainly introduces the topic selection, the main theoretical significance of this topic, and puts forward the research questions. Also the review of Chinese and Western literature provides useful reference for my further research. The third methodology part, introduced the research method, the choice of the theory, the choice of data, thesis structure and some limitations. The fourth part focuses on three theories used to analyze Sino-US cyber security: interdependence theory, national interest theory, and world system theory. The fifth part takes advantage of the fact that the two cases reflect the competition between Sino-US cyber security, highlighting the actions and strategies taken by the United States to maintain its hegemonic interests in cyber security. The sixth part is a political and economic analysis of Sino-US cyber security. With the change of dominant production factors, cyber security plays an increasingly important role in promoting economic development, which can guarantee the sound operation, technological innovation and economic security of the institutional environment. Under the increasing mutual distrust and fierce competition that China and the United States have formed, the United States must try to maintain its hegemonic status, and China is trying to rise in the current international system in which the United States is

dominant. The two countries will certainly play the game of interest in cyber security. Finally, the seventh part answers the research questions and draws conclusions.

### **3.5 Limitation**

The limitation of research in this thesis is, first, the difficulty in data collection and selection. Because the objects studied in this thesis have certain confidentiality, this increases the difficulty of collecting relevant materials. In addition, due to the limitations of the author's ability, the study of the network relationship of large countries in cyberspace has to limit the scope and subject, and confine the big country to China and the United States. In fact, in the cyberspace is not just a simple two-party game between China and the United States, but more commonly a multi-party game.

Secondly, this thesis mainly adopts qualitative research in research, but the research on the spatial relationship between China and the United States needs a certain quantitative research to support the arguments. It is necessary to use data to quantify the state of cyberspace relations between China and the United States. However, due to the limitations of realistic conditions, qualitative research methods are mainly used in thesis writing, but there are still insufficient quantitative empirical investigations.

## 4. Theory

### 4.1 Interdependence theory

Interdependence theory is an important theory that inherits the liberal political and economic tradition. In the late 1960s and early 1970s, there were some essential changes in the international community, there are trade protectionism caused by the disintegration of the Bretton Woods system, the confrontation of oil-exporting countries with oil as a weapon against Western countries, and the stagflation of the global economy. In this context, the theory of interdependence arises. Although it was proposed in various forms in the late 1960s, the theory of interdependence was systematically introduced in the 1970s. The main representatives and works are: Richard Cooper's "The Economics of Interdependence: The Economic Policy of the Atlantic Community", "Power and Interdependence" by Robert Keohane and Joseph Nye, Edward Moss, "Modernization and the Transformation of the International System".

There are many different definitions of the concept of interdependence, but scholars generally accept the definition of "power and interdependence" by Robert Keohane and Joseph Nye: "In general, dependence refers to a state that is dominated by or influenced by external forces. In short, interdependence is dependent on each other. Interdependence in world politics refers to situations characterized by interactions between actors in different countries or countries."<sup>13</sup>

Before the emergence of interdependence theory, realism theory occupied an absolute monopoly position. In the eyes of interdependence, the three most basic assumptions of realist theory: The state as the most important actor on the international stage is the determinant of international politics, the effectiveness of military means, the high-level politics governs low-level politics. These three assumptions can all be refuted. Interdependence believes that: First, the diversity of social communication channels, these channels are no longer limited to the

---

<sup>13</sup> Robert Keohane, Joseph Nye: "power and interdependence", third edition, 2001, p9.

relationship between countries, but also the links between international organizations, multinational companies and individuals. Second, the division between the issues is gradually disappearing, military security is not always the first issue among national relations, many issues are caused by domestic policies. In this way, the distinction between domestic issues and foreign policy issues is increasingly blurred. Third, military power no longer plays a leading role. In the case of interdependence, military power is not always regarded as a means of opposing another country.<sup>14</sup>

The development of information technology has promoted the deep development of globalization, the interdependence of political, economic, military and humanities among countries around the world has deepened, but interdependence does not mean mutual benefit or non-zero-sum game or equality.<sup>15</sup> In real international relations, national interests are still the preferred factor in each country's foreign policy formulation process, but the international mechanisms in the interdependent world system play an important role, we refer to a series of control arrangements that affect interdependence as international mechanisms.<sup>16</sup> The international mechanism has the role of compulsory, supervisory, and punitive, and there are many games in the state exchanges. Therefore, considering the long-term interests of the state, the state will still consider cooperation to promote the realization of interests among countries.

When analyzing the topic of cyber security in China and the United States, we need to recognize the beneficial effects of the network on the globalization process, the global economy, and the development of inter-state relations. However, due to the inherent shortcomings of cyber security, some countries, enterprises or individuals often use unfair means to obtain benefits under the influence of interests. But it is undeniable that the network plays an important role in the interdependent world formed by the flow of capital, technology and labor among countries. Network security directly affects Sino-US relations in an interdependent world and affects the stability and development of the two countries.

---

<sup>14</sup> Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010, pp 23-28.

<sup>15</sup> Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010, pp 118-119.

<sup>16</sup> Robert Keohane, Joseph Nye: "power and interdependence", third edition, 2001, p19.



## 4.2 National interest theory

In the international system, the state has important national interest objectives such as safeguarding national security and domain integrity, promoting economic development and social prosperity, and enhancing its international status and international influence. The most important thing in the theory of national interests is the national interest. The concept of national interest is considered a historical concept. According to research, the history of using interests as a guideline for diplomatic conduct can be traced back to the earliest period of the formation of the country in the 16th and 17th centuries, first in Italy, then in England.<sup>17</sup> According to Mark R. Amstutz, "In terms of its subjective characteristics, the national interest is based on the long-term collective interests recognized by all citizens of the country. Therefore, although the state pursues various foreign policies in the global system, the concept of national interests is a single and as a whole concept."<sup>18</sup> It can be seen that the interests of only one social sector cannot be regarded as national interests. The national interests should be the interests shared by the rulers and the ruled. It is the most important and highest priority shared by all sectors of the country in a certain period of time. Frederic S. Pearson and J. Martin Rochester point out that the national interests of sovereign states generally have at least three basic elements: First, to ensure their own survival, including protecting the lives of their citizens and maintaining territorial integrity; second, promoting the economic welfare and happiness of their people; and third, maintaining the self-determination and autonomy of their government systems. These constitute the core values of the country and the most basic foreign policy objectives.<sup>19</sup> These three elements are among the most important things in the national interest.

Power is an effective means of realizing national interests. The first issue discussed by Hans J. Morgenthau in his book "Politics Among Nations — The

---

<sup>17</sup> Rozeta E. Shembilku: "The National Interest Tradition and the Foreign Policy of ALBANIA", Master of Arts in Law and Diplomacy thesis, April 23, 2004, p. 6.

<sup>18</sup> Mark R. Amstutz: "International Conflict and Cooperation", Boston: Mc - Graw Hill, 1999, p. 179.

<sup>19</sup> Frederic S. Pearson, J. Martin Rochester: "International Relations", 4<sup>th</sup> edition, New York: McGraw- Hill, 1998, pp.177- 178.

Struggle for Power and Peace ", is that political power is a means of achieving national goals. Proposing that "national politics, like all other politics, is also a struggle for power. Regardless of the ultimate purpose of international politics, power is always the immediate goal. But as long as they seek to achieve their goals through international political means, they must always strive to expand their power. "<sup>20</sup> This shows that power is the means by which the state achieves its political goals. National interests are important political goals pursued by the state. Therefore, power is the means to realize national interests. What is the means by which the state pursues power? Morgenthau pointed out that it depends on strength, that is, the power of the state itself. He divides state power into two kinds: tangible and intangible. In both of them, Morgenthau sees intangible power more than tangible power. " Diplomacy can be said to be the brain of state power, and national morale is its soul."<sup>21</sup>

When analyzing the cyber security competition between China and the United States, the viewpoint of using the theory of national interest is more about considering national interests. Under the international system of anarchy, national interests are always a national priority. For a hegemonic power like the United States, hegemonic status gives it the greatest security, the highest prestige, and the most resource wealth gains. Therefore, the hegemonic power is the country that maintains the status quo, and its national interest is to maintain and consolidate such a position. For a big country like China, what they hope for is to seek a better position of the international system on the basis of the existing one. Such an international system is not based on delusions, but based on a correct understanding of the reality. Therefore, China's national interests in cyber security should be a better, but reasonable, positional goal, weaken strong opponents in the competition, and strive for a more powerful position. It can be seen that because of the structural conflicts between the national interests of the big powers and the interests of the hegemonic powers, there is a potential tension between the strategic interests of the two countries, especially the big countries are

---

<sup>20</sup> Hans J. Morgenthau: "Politics Among Nations — The Struggle for Power and Peace", Beijing: The Commercial Press Press, 1993.

<sup>21</sup> Hans J. Morgenthau: "Politics Among Nations — The Struggle for Power and Peace", Beijing: The Commercial Press Press, 1993.

not only close to the hegemonic power in terms of strength, but also challenge the hegemonic power in the system. Then it makes sense to use the theory of national interest to analyze the cyber security competition between China and the United States.

### **4.3 World system theory**

As a theory and analytical method, the theory of world system first emerged in the 1970s. The main symbol is Emanuel Wallerstein's "The Modern World System (Vol. I), 1974: Capitalist Agriculture in the 16th Century and the Origin of the European World Economy." The rise of world system theory is the synergy of multiple factors. Dependency theory precedes the emergence of the theory of the world system and becomes the source of academic thought in the later world system theory.<sup>22</sup> The social reality of the world system theory mainly includes the rise of the nationalist movement, regional integration, and the formation of the Cold War bipolar pattern. The theory of the world system attempts to analyze the evolution of the world system with the international system as the unit of analysis and the dependency relationship between the central fringe countries, the international division of labor and class conflict as research variables.

The world system theorists generally believe that the world system was born in Europe in the 16th century.<sup>23</sup> Geographical expansion, specialization of economic space, and the emergence of state machines are all reasons for the emergence of the world system. After the emergence of the world system, there are central and marginal areas. "The center uses state-of-the-art technology, the highest level of mechanization and the most intensive capital to produce the most advanced products. The situation on the edge is basically the opposite of the center, the technical level of economic activities is relatively backward, tending to be labor intensive, and exports are mainly concentrated in raw materials and agricultural products. The semi-edge is between the

---

<sup>22</sup> Wang Zhengyi: "World System and China", The Commercial Press, 2000, pp 42-44.

<sup>23</sup> Terrence K.Hopkins and Immanuel Wallerstein, eds.,World-Systems Analysis: Theory and Methodology, Sage Publications,1982, p.47.

center and the edge, its economic activity has both a central feature and a typical edge feature, the technical level and capital intensity are between the center and the edge.”<sup>24</sup>“The development process of the world economy tends to widen the economic and social gaps between different regions... In the entire history of the modern world system, the various advantages of the central countries have been expanding.”<sup>25</sup>

The center and semi-edge of the world system are not static, there are several development trends: the central countries may become semi-marginal countries, the semi-marginal countries may become marginal countries, the marginal countries may become semi-edge or core countries. In the process of development, marginal countries may become either central countries or marginal countries.

When analyzing the cyber security competition between China and the United States, the world system theory provides a useful reflection. The analysis units of interdependence theory and national interest theory are all countries, and the analysis unit of the world system is the world system. Such a perspective helps to understand the position of China and the United States in the world system because it directly affects the country's strategic intent and ability to act. In the world system, the United States is at the center of the world system. Although China's economic and social development has continued to develop over the past 30 years of reform and opening up, the position of the world system has been constantly changing, moving from the edge to the center, the most prominent is China's growing national strength and changes in the role played by world economic relations, but China is still in the stage of dependency accumulation and is still exploited by capitalist unequal exchanges. The development momentum of the world system is endless capital accumulation. The United States, which is at the center of the world system, is in a leading position in terms of capital and technology. China is still in the stage of attachment to the United States, and the United States will continue to carry out capital accumulation in

---

<sup>24</sup> Jiang Hua: "Theory of World System Theory: Centered on Wallerstein", Shanghai Sanlian Bookstore, 2007, p 79.

<sup>25</sup> Emmanuel Wallerstein: "The Modern World System (Vol. I): The Origin of Capitalist Agriculture and the European World Economy in the 16th Century", 1997, pp 215-224.

order to maintain the development of the world system. As a tool and purpose, cyber security competition plays a very important role in promoting the accumulation of capital in the United States, and it also plays an important role in the development of the international system.

## **5. Case analysis of Sino-US cyber security competition**

Since President Obama's took office, Sino-US network competition has erupted, and security conflicts have occurred frequently. It can be divided into two main categories: one is the conflict caused by the US accusation against China, and the other is the direct confrontation caused by the emergency. The US media speculation "China Hacker Base Camp" (2011.6), the United States identified Huawei and ZTE as cyber espionage activities (2011.2.11), the United States claims that Chinese hackers have stolen a large amount of US defense military information (2012.3.27) and the "Mandiant report" (2013.2.18), which are all accusations of US public opinion against China, the Chinese side has also made a strong counterattack and resolutely refused to accept such unwarranted speculations and accusations from the United States. The subsequent Snowden incident triggered the Sino-US cyber attack accusation (2013.6.22), the United States sued China's five military network hacking (2014.5.20), the US threatened sanctions against China cyber attacks (2015.4.1), the US class action lawsuit Lenovo Group illegal personnel invasion leads to information security risks (2015.4.2), the United States twice threatened to retaliate against Chinese cyber attacks and the United States sanctioned five Chinese companies due to hacking issues is a direct confrontation (2015.8.31).

In these cases of cyber security competition, I chose two cases, one is the prism gate event at the national level. Through the analysis of the prism gate event, it reflects the political and economic thinking of the United States in cyber security. The other is at the enterprise level, the event that China's two major communication service providers, ZTE Huawei, were investigated and blocked in the United States. The ZTE Huawei incident also reflects the game between China and the United States based on national interests in cyber security and the impact of interest groups on national cyber security policies.

## 5.1 Prism gate event

In June 2013, the British "Guardian" and the US "Washington Post" successively released information on the "Prism" plan provided by former CIA employee Edward Snowden. The former claimed that the United States collected 3 billion pieces of electronic information through the server only in March, and the latter directly named nine Internet giants including Google, Microsoft, Yahoo, Apple, Facebook and YouTube. The National Security Agency and the FBI can directly access the network company's central server to monitor the target's Internet access, including email, social tool chats, photos, audio, video, files and more.

The exposure of the Prism program has aroused strong repercussions in the United States. The public strongly opposes the government's collection of non-threatening personnel information and invasion of privacy. People refute Obama's remarks about preventing problems before they happen. They voted on the White House website to stop the Prism program and get a lot of people's response. After the incident, the United States admitted to the implementation of the Prism program, but they have defended the plan. Keith Alexander, director of the US Home Security Bureau and director of the Network Command, said that the plan only targets terrorism. It has protected the United States 50 times and can prevent more than 90% of the terrorist threat. National Security Adviser Tom Donilon was asked at the press conference how does the Prism program protect the target from pointing to non-Americans, he said that "the US government's monitoring plan is carried out in accordance with Article 702 of the Intelligence Collection Law. Unless there is an emergency in which someone wants to steal state secrets, ordinary people will not be involved in the plan."<sup>26</sup> White House spokesman Jay Carney mentioned Snowden at a press conference in July. "As a US citizen, Snowden is subject to US law and should return to the United States for appropriate treatment."<sup>27</sup> In November, Obama also

---

<sup>26</sup> The White House, Press Briefing by National Security Advisor Tom Donilon, June, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon>.

<sup>27</sup> The White House, Press Briefing by Press Secretary Jay Carney, July, 2013, <https://obamawhitehouse.archives.gov/photos-and-video/video/2013/07/16/press-briefing#transcri-pt>.

insisted that "although the US network is running smoothly, thousands of people log on to the website and apply for medical health services. What the government can do now is to ensure network security through political prisms. "<sup>28</sup>

However, things didn't get better. On March 24, 2014, Snowden once again disclosed that the US National Security Bureau has carried out large-scale network monitoring and stealing activities on targets such as Huawei, China's former leaders, the Ministry of Foreign Affairs, the Ministry of Commerce, and the banking system.<sup>29</sup>

In the past few decades, the rapid development of information technology has greatly changed the way of production and lifestyle of human beings. With the network as the link, a series of industries and departments including infrastructure, electricity, aviation and national defense are closely connected. Between countries, international exchanges have become more frequent and closer, and weaving into a close network. The relationship between China and the United States is also constantly evolving in this interdependent world. But why does the US want to monitor China? Among the targets of surveillance, there are national government departments, as well as Chinese companies like Huawei. Why does the United States want to monitor Chinese companies?

Why does the United States want to monitor China? As the only superpower in the world, the United States has the most advanced level of science and technology. China is the second largest economy in the world, and its economic development rate far exceeds that of the United States. In order to safeguard the status of the US hegemonic power and the interests of the hegemony, the United States must adopt corresponding means to maintain its interests under the conditions that technology can be realized. However, when analyzing cyber security, it should be noted that the United States also monitors its allies, such as Germany, France, Canada, Australia, etc., and the United States is also doing this for its national interests. Obviously, it is

---

<sup>28</sup> The White House, Remarks by the President at Second Joint DCCC/DSCC Event – Beverly Hills, CA, November. 2013.  
<https://obamawhitehouse.archives.gov/the-press-office/2013/11/26/remarks-president-second-joint-dccc-dscc-event-beverly-hills-ca>.

<sup>29</sup> Xinhuanet: "Snowden exposes the inside story of the US large-scale dialogue network attack", March 24, 2014.  
<http://news.xinhuanet.com/2014/0324/364972.shtml>.



generally believed that the US's monitoring behavior is to protect its national interests and cannot fully explain the behavior of the United States.

Among the targets of surveillance, there are national government departments, as well as Chinese companies like Huawei. Why does the United States want to monitor Chinese companies? For example, banking systems, Huawei companies, etc. The US National Security Agency has no reason to use its advanced technology to monitor Chinese companies. Surveillance of the government may be to obtain the corresponding intelligence and maintain its national security, but monitoring the true intentions of the company is obviously confusing. Although the United States claims that its monitoring of Chinese companies is not for commercial interests, it does not guarantee that it is not to consolidate its leading position in technology. The United States seeks to lead a new round of information technology change and continuous innovation of cutting-edge technologies. In this way, it will promote the growth of the US economy, ensure the US global economic hegemony, and consolidate the US's dominance in the world.

In the next chapter, I will conduct an international political and economic analysis of Sino-US cyber security, and analyze the cyber security game between China and the United States from a political and economic perspective, which will help to better understand the US monitoring of Chinese government departments and enterprises in the prism gate event.

## **5.2 ZTE Huawei event**

On October 8, 2012, the US House of Representatives Permanent Intelligence Committee issued a report for Chinese communications operators ZTE and Huawei, which was completed in 11 months.<sup>30</sup> The report alleges that the two companies' production operations in the United States and products threaten the security of US

---

<sup>30</sup> U.S. House of Representatives 112th Congress, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, October 8, 2012, [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf).

communications, and also pose a serious challenge to US national security. This report not only recommended that the US government prohibit the two companies from gaining access to sensitive US systems, prohibiting ZTE from acquiring US assets, but also recommending that governments and companies avoid using the equipment they produce. The US House of Representatives Permanent Intelligence Committee is an important legislature. Although its report is not mandatory, its strict wording and targeted recommendations have brought serious negative impact on the expansion of ZTE Huawei's two companies in the US market. Moreover, other governments and enterprises in other countries have expressed their support for the US investigation and intend to restrict the overseas development of ZTE Huawei. Once the report was released, it was immediately opposed by Huawei. Huawei said in a statement that the US House of Representatives Permanent Special Intelligence Committee failed to provide clear information or evidence to justify the report of the committee.

This is not the only investigation conducted by the US House Intelligence Committee against ZTE Huawei. Since November 2011, the Intelligence Committee has launched a series of unclear investigations on ZTE Huawei on the grounds of US national security. For example, investigate whether ZTE Huawei is controlled by the Chinese government, party organizations within the enterprise, the essential relationship between companies and so on.

From the point of view of the US national security threat, the US Foreign Investment Committee prohibits any acquisition or merger activities involving ZTE Huawei. It is recommended that the US government prohibit the two companies from gaining access to sensitive US systems and prohibiting their acquisition of US assets. It also recommends that the government and enterprises avoid using ZTE's equipment.<sup>31</sup> The U.S. House of Representatives' Standing Intelligence Committee issued such a report with apparently another attempt. The report stated that ZTE

---

<sup>31</sup> U.S. House of Representatives 112th Congress, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, October 8, 2012, [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf).

Huawei threatened its national interests without evidence. Why is the US House of Representatives Permanent Intelligence Committee doing such a report because of the national cyber security considerations of the United States or the protectionism of trade generated by domestic interest groups? The US government may exist for cyber security reasons because it mistakenly believes that the Chinese background of ZTE Huawei must be linked to national interests and confuse corporate interests with national interests. At the same time, it is worried that ZTE Huawei's large-scale development in the United States will not be conducive to the protection of intellectual property rights, and it will weaken the competitiveness of US-based companies. Both are not good for the United States.

As a typical representative of China's high-tech manufacturing enterprises, ZTE Huawei started from China and continued to expand into the markets of developing countries, and then entered the high-end market in Europe and America. The development of ZTE Huawei in the United States is not very smooth. Since the US company Cisco sued Huawei for infringement of intellectual property rights in 2003, Huawei has been competing with Cisco. In 2012, Cisco accused Huawei of stealing commercial documents. In short, the competition between Huawei and Cisco is accompanied by the development of two companies and involves the US government. For example, the US government has repeatedly blocked Huawei's corporate mergers and acquisitions in the United States. The US government claims that ZTE Huawei threatens US communications security. Are these acts of the United States and the investigation by the US House of Representatives Permanent Intelligence Committee the result of Cisco lobbying behind the scenes? As a result, Cisco can reduce competition and achieve greater profits in the United States.

In the analysis of ZTE Huawei's investigation in the United States should not only be considered from the perspective of its domestic politics and interest groups, but also should take into account the factors of national power. Between China and the United States, the changes in state power clearly show that China has an advantage. The United States is also a factor that should be taken into consideration in order to safeguard its economic development and the purpose of global hegemony.

## **6. Political and economic analysis**

The change of production factors affects the creation of social wealth. As a production factor, the rise of the network has shaped a new type of world economy, which in turn affects the growth of international wealth and the country's development strategy. While shaping the new world economy, the network has also strengthened the relationship between economic growth and cyber security. Cyber security affects institutional environment, technological innovation, economic security and other factors, and these factors are directly related to economic development. As the world's only superpower, the United States seeks to maintain its global leadership by achieving economic development. As the world's second largest economy, China also needs to maintain sustained economic growth to maintain domestic social stability. However, as the status quo in the modern international system, the United States has to maintain its global hegemony status, and China, as an emerging rising country, tries to change the existing international political and economic order, which is more conducive to the realization of national interests. As a field of Sino-US game, cyber security will have a profound impact on the relationship between the two countries. Therefore, it is of great practical significance to conduct political and economic analysis of Sino-US cyber security.

### **6.1 Global network and new world economy**

#### **6.1.1 Changes in factors of production**

In economics, the factor of production refers to the resources used to produce goods or provide services, and is a basic category in economics.<sup>32</sup> At different stages of production development, the dominant factors of production are constantly changing. Traditional production factors mainly include land, capital, and labor, but modern Western economics regards entrepreneurs as a production factor.<sup>33</sup> With the

---

<sup>32</sup> Freeman: "Labor Regulations and Social Protection in Developing Countries: Market Distortions or Efficient Institutions? ", NBER Working Paper No. 14789, 2009.

<sup>33</sup> Cao Jianping: "Political Economic Analysis of the International Flow of Production Factors——Based on the Perspective of Global Production Network", International Economic and Trade Exploration, 2013.

development of science and technology, information and technology are also put into production as relatively independent production factors. By combining the changes in the dominant factors of production in the process of economic development, we can more clearly understand what is the dominant factor of production in a certain period and dominate the creation of social wealth and economic development. Changes in factors of production can be divided into three main stages: First, land dominates the stage of production factors, land has always been the most important factor of production before the rise of capitalism. Second, capital dominates the stage of production factors, after the capitalist business and credit system, capital began to play an important role in promoting economic development as an important factor of production. Third, science & technology and management dominate the stage of production factors, especially after the information technology revolution, production factors have also undergone great changes, and science & technology play an increasingly important role in factor allocation.

#### **6.1.1.1 Land dominates the stage of production factors**

In the early days of human society, agriculture was the foundation of a country, and the most important land for agriculture was invested as the most basic means of production in self-sufficient agricultural development. There is a very big difference between the land-occupying farmer and the landless person. In order to survive, the landless people only depend on the landowner and lose their freedom of life. Under the feudal serfdom, the aristocratic class owned the land, and the slave status was low, serving the feudal lords and aristocratic classes. The physiocratism before the emergence of mercantilism emphasized the importance of agriculture, considering agriculture as the sole source of wealth and the basis of social income.<sup>34</sup> There must be land for the development of agriculture, and there is no point in developing agriculture without land. Therefore, in the primitive accumulation stage of capitalism, the landlords will separate the peasants from the production materials such as land

---

<sup>34</sup> Cao Jianping: "Political Economic Analysis of the International Flow of Production Factors——Based on the Perspective of Global Production Network", International Economic and Trade Exploration, 2013.

through violent means. In primitive society, slave society, and feudal society, land is a dominant factor of production. In modern society, although land is not the dominant factor of production, land is still one of the most important factors of production.

#### **6.1.1.2 Capital dominates the stage of production factors**

Geographical discoveries, with the establishment of banking and credit systems and the rise of early trade, capitalist society began to have early capital accumulation, but at this time capital is not the dominant factor of production. Until the middle of the 18th century, capitalist factory handicrafts became the main mode of production, and capitalists also shifted from primitive accumulation to capital accumulation. Capital accumulation is based on the deprivation of surplus value.<sup>35</sup> After acquiring the surplus value, the capitalist expands the production needs in pursuit of high profits, instead of satisfying the individual needs of the capitalists, but invests in new production, so that the surplus value is transformed into capital. In the early 20th century, the emergence of monopoly organizations, the emergence of financial oligarchs, the input of capital, and the division of the world by capitalists, all of which were generated by the dominant role of capital. In this period, capital replaced land as the dominant factor of production.

#### **6.1.1.3 Science & technology and management dominate the stage of production factors**

In the history of human civilization, there have been three scientific and technological revolutions. Following the steam revolution and the power technology revolution, the third revolution in the field of science & technology has greatly changed the way of life and production. It is a technological revolution in information control, with the invention and application of atomic energy, space technology and biotechnology as the main symbols, as well as new energy technologies, information technology and many other fields. Its most direct impact is to cause changes in the factors of production, so that labor productivity has increased significantly, and at the

---

<sup>35</sup> Cao Jianping: "Political Economic Analysis of the International Flow of Production Factors——Based on the Perspective of Global Production Network", International Economic and Trade Exploration, 2013.

same time, the economic structure has undergone a very big change. The reason why management can dominate the production factors is mainly because the production efficiency of modern enterprises is greatly improved in the organization and management of enterprises, especially the professional manager revolution.<sup>36</sup>

After analyzing the changes in production factors, it can be clearly seen that the dominant production factors are from land to capital to science & technology and management. The network is closely related to the production factors that are now dominated. As the most important technology for the development of science & technology, its impact on human social life is not a unilateral or certain aspect, but a global impact. Network technology dominates modern science & technology, and natural network technology can also be the dominant production factor. Because of the production and life of modern human beings, the creation of wealth has been difficult to break away from network technology.

### **6.1.2 Interdependence of the network and the new world economy**

The change of production factors affects the creation of social wealth. The rise of the network as a production factor shapes a new type of world economy, which in turn affects the growth of international wealth and the development strategy of the country. The international economy is very different from the present before the network does not appear or the network is not put into production as a factor of production. The generation of the network and the input of network production factors closely connect global production, exchange, and sales, and have a great impact on specific areas of the international economy, such as typical international trade, international investment, international finance, national development and other fields.

With the application and rapid popularization of network technology, e-commerce has achieved unprecedented development in both breadth and depth, and penetrated into all aspects of society. As a network-based exchange method,

---

<sup>36</sup> Cao Jianping: "Political Economic Analysis of the International Flow of Production Factors——Based on the Perspective of Global Production Network", International Economic and Trade Exploration, 2013.

e-commerce has become an important domestic and international trade. E-commerce has reduced many traditional trade links, and has the advantages of wide customer coverage, large coverage, fast delivery of information, low price, and quick and easy transaction.<sup>37</sup> Its development speed will be faster and faster, it has become a key driving force for world economic growth, and has a profound impact on international trade. Similarly, the Internet has a very large impact on finance, which has promoted the emergence of Internet finance. It plays a huge role in promoting financial development and prosperity and stimulating economic growth. In terms of international investment, the network plays an important role in reducing transaction costs, ensuring information transparency, and symmetry of information. In terms of national development, the network, as a factor of production input, integrates the primary, secondary and tertiary industries, improves production and service efficiency, and accelerates the creation of national wealth. The development of the network has more or less impact on the international trading system, the international financial system, and the country's development strategy. According to the hypothesis of interdependence theory, the network has shaped an emerging world economy. In the world economic system, various actors, including the World Trade Organization, the World Bank, the International Monetary Fund and other national actors, including non-state actors such as multinational corporations, have formed an interdependent relationship, the network is the driving force for its development and change.

The new world economy is characterized by interdependence. In an interdependent world economy, the economies in which actors are interdependent are sensitive and vulnerable. Sensitivity is mainly manifested in the speed at which a change in one actor in a new world economic system leads to a change in the cost of another actor. The faster the speed, the greater the price paid. Vulnerability is manifested as the loss suffered when the link between actors is cut off.<sup>38</sup> The new global economy, whether sensitive or vulnerable, is more vulnerable than the previous

---

<sup>37</sup> Nicholas Westcott: "Digital Diplomacy: The Impact of the Internet on International Relations", Oxford Internet Institute, 2008.

<sup>38</sup> Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010, p. 119.



world economy. The network plays an important role in shaping the new world economy. The role of the network in the formation and development of a new world economy is equally important. The network plays a role in safeguarding and promoting the formation and development of a new world economy. The promotion is well understood, that is, as an input of technical factors, it promotes the development of the economy. Safeguard is related to cyber security issues. Once the network security problems in the fields of global e-commerce and Internet finance are problematic, it will have negative impacts that are difficult to imagine.

Network technology has shaped a new world economic system that is interdependent. At the same time, the stability of the new world economic system requires cyber security as a foundation guarantee. In the new world economy shaped by the Internet, the interdependence between China and the United States has achieved unprecedented development. In addition to China and the United States, multinational corporations and people of both countries play a very important role in the development of bilateral relations. Although the gap between China and the United States is further narrowing, the military is no longer a priority for the United States to safeguard its interests, because the diversity of the channels of communication in the interdependent world is not a game in China and the United States, but there are multiple games, any betrayal and free-riding behavior will affect the national interest. The stability of the new world economic system requires cyber security as a basic guarantee. If cyber security is not guaranteed between China and the United States, in the interdependent Sino-US relations, cyber security issues will spread to other issues, which will have a huge impact on the economic development and social stability of China and the United States.

## **6.2 Cyber security and economic growth**

While shaping the new world economy, the network has also strengthened the relationship between economic growth and cyber security. Network security affects institutional environment, technological innovation, economic security and other

factors, and these factors are directly related to economic development.

### **6.2.1 Institutional environment**

When analyzing the impact of the institutional environment on economic growth, we first think of a long-term discussion that has plagued economic history and the history of science & technology. The three technological revolutions are all about Europe and the United States. Why is it not with China? The academic community has been discussing this issue for a long time, but the conclusion is not convincing.

Later, the American institutional economics scholars North and Thomas analyzed that the scientific & technological revolution did not occur in China mainly because China lacked a corresponding institutional environment. The institutional environment stimulates social innovation, and social innovation requires an appropriate institutional environment to produce. In the analysis, North and Thomas believe that the system guarantees that the private benefits of innovators are close to the social benefits generated by innovation. Innovators will consider the cost-benefit problem from a personal perspective. If the products developed after the investment in the society cannot offset the cost, natural innovation will not occur. On the contrary, if the benefits far outweigh their costs, innovation will arise. Individual cost-benefits take into account the revolutionary changes in science and technology. This is not to say that the only criterion for the quality of the institutional environment is to stimulate innovation. A good institutional environment should take into account social freedom and publicity while maintaining efficiency.

The institutional environment analyzed here is mainly to more clearly illustrate the relationship between cyber security and the institutional environment. How cyber security affects the institutional environment, which in turn affects economic growth, is our focus. The definition of institutions is complex, and here we consider institutions to be the basic political, social, and legal rules used to establish the basis of production, exchange, and distribution.<sup>39</sup> The most important institutional

---

<sup>39</sup> Douglas North, Lance Davis: "Theory of Institutional Change: Concepts and Causes", in Ronald Kos: "Property Rights and Institutional Change: A Collection of Property Schools and New Institutional Schools", 1991.

environments include intellectual property, patents, trade secrets, copyrights, etc. But today, as the network grows, the network has become closely related to all aspects of society. It is very important to ensure that the institutional environment protected by intellectual property, patents, trade secrets, copyrights, etc., operates effectively.<sup>40</sup> The improvement of intellectual property rights, patents, trade secrets and copyrights can stimulate more people to actively participate in innovation, because in this case, innovators take into account the cost-benefit of innovation and believe that the benefits can offset the cost of their innovation inputs, therefore, protecting the institutional environment dominated by intellectual property rights is conducive to technological innovation and thus to economic growth.

While ensuring cyber security between China and the United States, it can also prevent individuals in any of the two countries from stealing commercial secrets and other commercial crimes and hacking attacks through the Internet. Once there is a problem with cyber security in China and the United States, it brings incalculable losses to the economic security and economic development of the two countries.<sup>41</sup> In a good institutional environment, cyber security is guaranteed by legislative means or other corresponding technical means, and intellectual property rights are also protected to some extent. This is very important for both China and the United States economic development. Only when the institutional environment is protected can the economy achieve healthy and sustained growth.

### **6.2.2 Technological innovation**

From the economic history since the 18th century, technological innovation has become the driving force of economic growth, and its role has exceeded the contribution of other factors of production such as capital, land, and labor to the growth of economic growth. Technological innovation has become the engine of

---

<sup>40</sup> Barrientos: "Corporate Purchasing Practices in Global Production Networks: A socially Contested Terrain", *Geoforum*, 2013.

<sup>41</sup> Kenneth Lieberthal, Peter W. Singer: "Cyber security and U.S.-China Relations", February, 2012, <http://www.brookings.edu/research/papers/2012/01/23-cybersecurity-china-us-singer-liberth-al>.

economic growth.<sup>42</sup> Technological innovation is the main means for a company to obtain lucrative profits, technological innovation is an important support for the country's macroeconomic regulation and control, technological innovation is also a driving force for the adjustment of the country's economic structure.

In 1956, the American economist Robert Solow established a new model of economic growth. In his model analysis, it was found that the contribution rate of capital production factors to the economy was not the most important. If there is no technological advancement, it will not be able to achieve sustained economic growth by increasing savings and increasing capital accumulation and investment. Solow believes that technological advancement includes not only the improvement of production technology in the usual sense, but also the improvement of production and commercial organization, and should include the improvement of the quality of labor brought about by the popularization of education.<sup>43</sup> Technological progress is an indicator that is difficult to quantify relative to production factors such as capital, land, and labor. But with the accumulation of experience, more and more people realize that technological progress is more conducive to economic growth than capital investment.

In an open economic system, technological innovation can drive the free flow of people and the free expansion of market scale. At the same time, technological innovation can ensure that the market fully exerts its automatic regulation function, and can also promote the establishment and improvement of the educational research system.

In the era of highly developed information technology, the innovation of information technology itself and the innovation of other industries guided by information technology as an instrumental means have the function of promoting economic growth.<sup>44</sup> Cyber security can guarantee the innovation of new technologies

---

<sup>42</sup> Nicholas Westcott: "Digital Diplomacy: The Impact of the Internet on International Relations", Oxford Internet Institute, 2008.

<sup>43</sup> Robert Solo: "Technology Change and Total Production Function", The Commercial Press, 1991, p. 2.

<sup>44</sup> Barrientos: "Corporate Purchasing Practices in Global Production Networks: A socially Contested Terrain", Geoforum, 2013.

and smoothly enter the market, creating national wealth. For example, in the Internet era, Internet finance is a financial innovation realized by the financial industry under the support of network technology. The most basic requirement of Internet financial operation is to ensure the security of its funds. Once there is a problem with the operation, the funds will be lost, which will likely impact the entire financial industry. The impact of the financial industry is likely to trigger a large-scale economic crisis.<sup>45</sup> Therefore, cyber security is crucial in technological innovation, especially the innovation of network technology itself and the innovation of related industries led by network technology. But no matter what, technological innovation is indeed a very important means to ensure economic growth. Cyber security is a means of guarantee, guaranteeing the emergence of innovation, ensuring the smooth production of the fruits of innovation and creating national wealth.

The United States has the strongest technological innovation capability in the world. Technological innovation plays an important role in the economic development of the United States. In the future development of the US economy, the United States will inevitably maintain its level of sustained technological innovation in order to maintain its leading position in the global economy. While cyber security is related to the ability of technological innovation and the transformation of technological achievements, the United States will be guaranteed in terms of cyber security to maintain its dominant position. Although China does not have the same technological innovation capabilities as the United States, in the process of Sino-US economic development, it has also paid more and more attention to the development of technology innovation, and cyber security will naturally become a problem that China has to face seriously. Cyber security is a global issue. It is not a problem that any country can solve alone. Only by working together can China and the United States create a harmonious cyber security environment. A good network security environment between China and the United States is conducive to technological innovation between China and the United States and is conducive to the economic

---

<sup>45</sup> Nicholas Westcott: "Digital Diplomacy: The Impact of the Internet on International Relations", Oxford Internet Institute, 2008.

development of the two countries. The implementation of the "beggar-my-neighbor" cyber security policy of any country is not conducive to the creation of a good cyber security environment, and is not conducive to the sustained and healthy development of Sino-US relations.

### **6.2.3 Economic security**

Economic globalization has developed rapidly, economic ties between countries have been continuously strengthened, and the status of national economic security in national security has become increasingly important. Especially with the development of information technology, information technology has connected all walks of life in the national economy. Economic security is the basis for ensuring economic growth, but in this analysis we mainly analyze how cyber security affects economic security, and economic security is at least a necessary condition for economic growth.

Economic security involves the security of the economic system, the security of the industry, and financial security.<sup>46</sup> Here is a brief analysis of how cyber security affects the security of the economic system, industry security, and financial security.

The security of the economic system can guarantee the stability of the country's macro economy and sustainable economic development. The emergence of the economic system is more artificial, based on domestic and foreign experience combined with the current domestic economic operation considerations to develop a series of policies. The system has the function of supervising the operation of the economy. When there is a problem with the cyber security, the supervision function of the system will be greatly reduced, and the economic operation will not be timely and accurately reported, resulting in instability of the economic system and thus affecting economic growth.

There are also such problems in industry security. The development of information technology and industry complements each other. On the one hand, it improves the production efficiency of various industries, on the other hand, it makes

---

<sup>46</sup> Zhang Shiquan: "Overall Research on National Economic Security", International Technology and Economic Research, 2003.

the dependence of various industries on information technology more and more strong. When cutting off the network, some industries, especially those closely related to information technology, such as information technology, e-commerce and other industries, once the network is obstructed or cut off, the entire industry will be paralyzed and unable to operate. Although some industries do not have such deep dependence on information technology as these industries, but information technology is an important guarantee for its operation and development. If there is a problem with cyber security, the development of the industry will bring great losses. In specific industry security, cyber security plays a very important role. Cyber security is the guarantee of its operation and the support of its development.

In the financial industry, the relationship between financial security and cyber security seems to be closer. Most of the current financial operations are operated on the Internet, which improves the efficiency of capital utilization and the rapid development of the financial industry, and also promotes the rapid development of the global economy. However, whether it is artificial cyber security or physical cyber security, it is likely to cause major changes in the financial industry. For example, on February 27, 1995, the British commercial bank Bahrain Bank closed down due to the wrong operation of a trader. As soon as the news came out, it immediately caused a sensation in Asia, Europe and the Americas. It also caused great damage to the financial community. This shows the fragility of the security of the modern financial industry. In addition, the gap between the developed and developing countries in the financial industry is also obvious. Developed countries can often create different financial derivatives in the market as a tool to control their financial hegemony. In the Internet age, developed countries will use their inherent advantages in the financial industry to launch an offensive against developing countries, forcing the corresponding countries to achieve financial liberalization. Once financial liberalization, developed countries can easily use financial weapons to defeat them. In the Internet age, it has accelerated the flow of finance and has also exacerbated the instability of the financial industry. This instability includes not only the instability caused by malignant technologies such as network intrusion, but also the instability

caused by financial stability in a country under legitimate competition.

Network technology has accelerated the pace of economic development. At the same time, cyber security issues may have a huge impact on economic security. If the cyber security problem in the process of economic development cannot be effectively controlled, the results of economic development are likely to disappear in a very short period of time because of cyber security problems, which will have disastrous consequences for the global economy. The focus of previous economic security concerns was mainly on the formulation and implementation of economic policies. Little attention was paid to cyber security. With the development of information technology, the network began to be invested as a factor of production in economic development, and economic security and cyber security are beginning to be closely linked. Only when the issue of cyber security is resolved can economic security be guaranteed.<sup>47</sup>

Sino-US cyber security also faces such problems in the economic development. China is a developing country, while the United States has its inherent economic and technological advantages.<sup>48</sup> It has sufficient strength to use its existing technological advantages to launch cyber warfare against China, which has a negative impact on China's economic security. In an interdependent world, both China and the United States are the community of destiny, but this does not mean that the United States will not have an impact on China's economic security because of its interdependence. From the perspective of national interest theory, in the game of cyber security, China and the United States must take the national interests as their starting point. In the cyber security competition, there is a certain tension in the national interest relationship between China and the United States. Whether it is acquiring the status of hegemonic power or acquiring the status of hegemonic system, China will pose a direct challenge to the national interests of the United States. In order to maintain its global hegemonic status, the United States will certainly make a difference in China's

---

<sup>47</sup> Ma Lin, Lei Jiachao: "Improve the system and institutional framework for maintaining national economic security", *Journal of Tsinghua University (Philosophy and Social Sciences)*, 2002.

<sup>48</sup> Stephen Roach: "Can China learn from American experience?", *Economic Globalization - Asia and China*, 2001, p 462.



economic security with the growth of China's economy and the expansion of its influence. In the Prism Gate Event mentioned in the previous chapter, one of the monitors was Huawei, a private enterprise in China. Through the analysis of network security and economic development in this chapter, we can see that the action of US monitor Chinese companies, its goal is to safeguard its national interests, safeguard its national security and economic development, and hope to learn more about China's economic information, especially in information technology resources, to ensure that the United States has always been in the leading position in the field of information technology. In order to realize China's economic development and national interests, China will also develop a series of cyber security strategies to ensure institutional stability, technological innovation and economic security.

To achieve healthy and stable economic development and maximize national interests, China must first ensure institutional stability, technological innovation and economic security that are closely related to economic development. In the process of economic development, cyber security is a problem that must be resolved first. Cyber security is directly related to the implementation of China's future economic strategy and the healthy and stable economic development.

### **6.3 Sino-US cyber security under the evolution of the international system**

Under the continuous evolution of the international system, Sino-US relations have also undergone constant changes. The status quo of Sino-US relations can be summarized as: increasing mistrust and fierce competition between the two countries. Despite the increasingly fierce competition between China and the United States, the interdependence between the two countries has also deepened. Driven by national interests, the United States seeks to maintain its global hegemonic status,<sup>49</sup> while China continues to rise, and cyber security, as an important area of the game between

---

<sup>49</sup> Wallerstein, Immanuel: "The Three Instances of Hegemony in the History of the Capitalist World-Economy", *Social Theory: Roots and Branches* edited by Peter Kivisto, Fourth Edition. New York: Oxford University Press, 2011.

the two countries, naturally has a very important impact. Also, in the international system, the United States has always been at the core of the international system, and China is shifting from the semi-edge to the core, and cyber security plays an important role in the process of transfer.

### **6.3.1 Sino-US relations under global competition**

China and the United States have established diplomatic relations for more than 40 years, and bilateral relations have developed into the most important and complex bilateral relationship in the world. The healthy development of Sino-US relations is beneficial to the interests of the two countries and their peoples, and is also conducive to the stability of the Asia-Pacific region and world peace and development. In the past 30 years, although China and the United States have more close dialogues and exchanges in the fields of economy and mutual visits, the increasingly close exchanges have not brought strategic mutual trust to China and the United States. On the contrary, there has been a crisis of confidence between China and the United States, and this mutual distrust has expanded.

Mutual distrust does not happen by chance. Its roots lie in the differences between the fundamental interests of the two parties and the judgment on the future development trend.<sup>50</sup> The reason for the growing mutual distrust between China and the United States is mainly because the two countries are not clear about the development trend of the other side and the differences between the two countries in terms of core interests. China and the United States are different because of the political system, ideology, historical and cultural traditions, and development status. This is also the reason for their differences. But the increase in mutual distrust is obviously not simply thought to be caused by the inherent differences between the two countries. If we think so, then the inherent differences will not change, or China will increasingly integrate into the modern world system, and Sino-US relations should tend to be better. But the opposite is true. The most likely understanding is the

---

<sup>50</sup> Jin Canrong and Dai Weilai: "Injecting Positive Energy into the Development of New Types of Great Power Relations between China and the United States - Analysis of China-US Strategic and Economic Dialogue", *Journal of International Relations*, No. 2, 2013.

change in the position of China and the United States in the world system in the past 30 years. Although the United States has always been at the core of the world system, China has shifted from the semi-edge to the center in the world system.

In the past 30 years, one of the most important things in China and the United States has been the rise of China. China's economy has developed steadily and rapidly, and in 2010 it became the world's second economy.<sup>51</sup> The gap with the US economy has further narrowed. At the current rate of economic growth in China, China's economic aggregate will surpass that of the United States in the near future and become the world's largest economy. And in these years, China's status and influence in the international community has also increased, and the will to defend national sovereignty and territorial integrity has become more determined, which has worried the United States. Worried that China's growing international influence along with the rapid economic growth will threaten the US's hegemonic position.

Another thing that has an impact on Sino-US relations is the relative decline in US power. Since the 9.11 attacks, the United States has launched the Iraq War and the Afghanistan War in the name of counter-terrorism. These two wars have brought the United States into war. In the global economic crisis in 2008, the United States suffered a long period of time after the crisis, the economic recovery was weak, the unemployment rate remained high, and economic growth was weak. Although China has also suffered from the economic crisis, the Chinese government has adjusted its fiscal policy, monetary policy and economic development mode in a timely manner. China soon emerged from the economic crisis and achieved stable economic development.

In recent years, cooperation between China and the United States has made positive progress in various fields, and at the same time, competition has become more intense. The United States has repeatedly exerted pressure on China on a series of issues, such as cyber security, trade, the RMB exchange rate, the DPRK nuclear issue, etc., and announced in 2010 a high-profile announcement of "returning to the

---

<sup>51</sup> Sun Tongqiang: "China Economic Report", Beijing: China Economic Publishing House, 2010.

Asia-Pacific region” with the intention of balancing China’s growing influence in the Asia-Pacific region. .

The status quo of Sino-US relations can be summarized as: increasing mistrust and fierce competition between the two countries. Understanding the status quo of Sino-US relations under global competition is conducive to a more objective and accurate view of cyber security and the development of Sino-US relations. Despite the growing distrust between China and the United States and the increasingly fierce competition between the two countries, with the promotion of network technology, production factors have changed correspondingly, shaping a new world economy. At the same time, the interdependence between the two countries has deepened. The interaction between the two countries is becoming more and more important in terms of linkage strategy, agenda setting, transnational and intergovernmental relations networks, and the role of international organizations. The relationship between the two countries has also become closer and closer. It is also because of such deep interdependence that the relationship between the two countries has become more sensitive and vulnerable due to cyber security. Changes between China and the United States, any country in the political and economic fields, may lead to another country's reaction, and may also pay a corresponding price.

The growing distrust and the increasingly fierce competition are a status quo between China and the United States. However, no matter how the position of China and the United States in the world system changes, there is a fact that China and the United States must build a new type of relationship between big powers, properly handle the contradictions between the rising and the defending countries, and cannot walk the old road of the rise and fall of big countries. China and the United States have many points of interest. China is the largest developing country with a large labor force and a vast market. The United States, as the largest developed country, has capital, advanced technology and management experience. China and the United States need to achieve a win-win situation, and China and the United States, which have benefited from the changes in network technology, are facing a development that is not conducive to the development of the two countries because of cyber security

issues.

### **6.3.2 Maintenance of the US hegemonic system**

After World War II, the United States became the only hegemonic country in the world.<sup>52</sup> Regardless of the basic strength model, the power action model, or the Marxist model, the United States has the power and prestige of hegemony, which dominates the global economic order and provides military protection for its allies. Although the US hegemony began to decline after the 1970s, with its political, economic, and military advantages, the United States is still the only super-state in the world.<sup>53</sup> The development of network technology brings new game forms and game content to China and the United States. Network security is one of them. In terms of cyber security, the interests of China and the United States are the game. The United States is mainly to maintain its hegemonic position in the world system. This hegemonic status mainly includes two aspects of hegemony: first, hegemony in the economic field; second, hegemony in the political and military field.

#### **6.3.2.1 Hegemony in the economic field**

Economic hegemony plays a very important role in the hegemonic position of the United States. If the economic hegemony of the United States gives way to other countries, political hegemony and military hegemony may also be loosened. If the US economic hegemony remains strong, then economic hegemony will support political and military hegemony, then the US hegemonic position in the world system will not be able to move and can continue more stably. However, since the financial crisis in 2008, the world's power has shifted from west to east, the US economy has been sluggish, and the domestic unemployment rate has remained high. In the international arena, especially international organizations such as the International Monetary Fund and the World Bank, on the one hand, the United States wants to maintain its existing

---

<sup>52</sup> Appelrouth, Scott and Laura Desfor Edles: "The Global Society in Sociological Theory in the Contemporary Era: Text and Readings", Thousand Oaks: Pine Forge Press, 2007.

<sup>53</sup> Collins, Randall and Michael Makowsky: "The Discovery of Society", eighth edition. Boston: McGraw Hill Higher Education, 2010.

interests, on the other hand, it tries to reduce its responsibility, which causes the international prestige and reputation of the United States to decline.

At a time when the US economy is weak and looking for an economic development strategy, information technology is taking a new round of changes, focusing on big data, cloud computing, and wearable devices. The United States has an advantage in information technology, and it must occupy a dominant position in a new round of economic transformation.<sup>54</sup> What is the relationship between cyber security and a new round of information technology change? Because the new round of technological change is mainly based on big data, in the era of big data, defining the boundaries of data is very important. In the implementation of data collection, not all data is public data, some involve privacy and national security, and these data cannot be collected. If data involving privacy and national security is protected, the development of big data will be somewhat limited. If these data are not protected, then national security is guaranteed. The United States has an advantage over China in information technology. The United States can guarantee its economic development by setting a series of international rules that are conducive to the United States itself in terms of cyber security. The rules enacted by the United States are likely to hinder China and other countries as a barrier to development.

Cyber security is related to the maintenance of US economic hegemony. It is also because the United States monitors China through its advanced technological means, such as the Prism Gate Event, and monitors China's Huawei and banking systems. The United States has a clearer understanding of China's information technology development and economic development trends by monitoring and illegally obtaining information on Chinese companies and countries. These behaviors in the United States are designed to maintain their position in the world system and prevent China from moving to the center of the world system.

---

<sup>54</sup> Zalmay M. Khalizad et al., *The United States and a Rising China: Strategic and Military Implications*, Rand, 2006.

### 6.3.2.2 Hegemony in the political and military field

On July 14, 2011, the US Department of Defense issued the "Network Space Action Strategy" report, which aims to strengthen the cyber security protection of US military and critical infrastructure, and the cyberspace is listed as the US military action field alongside the Army, Navy, and Air Force.<sup>55</sup> The release of the report shows the intention of the United States to expand its cyberspace. After the 9.11 incident, multiple computer systems of US federal agencies suffered cyber attacks. In order to prevent attacks by the network, the United States has established a network force to respond to cyber warfare. The network forces only need to use computer network technology to attack the other party's infrastructure and mobilize the command system in the network environment, resulting in the enemy being in a passive position.

The United States is a developed and leading network technology company that can interfere with China's internal affairs by virtue of its network technology. Since the Internet has no borders, the United States can infiltrate China and promote American values and American-style democracy. The United States can also interfere with China's military facilities and military development through the Internet, and control the development of China's military. Therefore, the relationship between the Internet and US political and military hegemony is easy to see. The purpose of the US investment in cyberspace is to maintain its hegemonic position in the political and military fields. The United States ensures its own cyber security, is not challenged and threatened by China, and maintains its hegemonic position in the world system. China also needs to ensure network security and cannot be passive to ensure China's political stability and military development.

The rise of the internet around the world has led to corresponding changes in the factors of production, shaping the new global economy and bringing the global economy closer together. China and the United States have also achieved political and economic development in the development of the network. However, because

---

<sup>55</sup> People's Daily Online: "The United States released its first <Network Space Action Strategy>" [http://paper.people.com.cn/rmrb/html/201107/16/nw.D110000renmrb\\_20110716\\_10-03.htm?div=-1](http://paper.people.com.cn/rmrb/html/201107/16/nw.D110000renmrb_20110716_10-03.htm?div=-1), July 16, 2011.

network technology has security problems, cyber security affects a country's institutional environment, technological innovation, and economic security. Therefore, cyber security has become more closely related to economic development. Under the assumption that "the country is rational", in order to maximize global interests, China and the United States are bound to take measures in cyber security to achieve their own development and limit the development of each other. As analyzed above, in the future when new technological changes are coming, if the United States wants to maintain its hegemony in the global economic field and political and military fields, in order to safeguard the national interests of the United States in the world, cyber security is a very important area. The interests in the field of cyber security are related to the interests of the US economy, political and military fields.

### **6.3.3 The rise of China in the world system**

After the reform and opening up, the Chinese economy has entered a new stage of development after more than 30 rapid developments, and has continuously integrated into the modern world system.<sup>56</sup> After the end of the Cold War, the United States intends to integrate China into the world economic system, but later, China gradually evolved from a passive participant in the world system to actively integrate into the world system.<sup>57</sup> Because China recognizes that isolated China cannot fully develop, China is gradually integrating into the world system and moving from the half edge of the world system to the center.<sup>58</sup> "The center uses state-of-the-art technology, the highest level of mechanization and the most intensive capital to produce the most advanced commodities. The marginal situation is basically the opposite of the center, and the technical level of its economic activities is relatively backward, tending to be labor-intensive, and exports are mainly concentrated on raw materials and agricultural products. The semi-edge is between the center and the edge. Its economic activity has both a central feature and a typical edge feature. The

---

<sup>56</sup> Jiang Hua: "Theory of World System", Ph.D. Thesis of Fudan University, 2003.

<sup>57</sup> David Scott: "The Chinese Century? The Challenge to Global Order", Hampshire: Palgrave Macmillan, 2008, P.14.

<sup>58</sup> "The Dangers of A Rising China", the Economist, Dec 2, 2010, <http://www.economist.com>.



technical level and capital intensity are between the center and the edge.”<sup>59</sup>

There are several development trends in the world system: central countries may become semi-marginal countries, semi-marginal countries will become marginal countries, marginal countries may become semi-marginal or core countries, In the process of development, the semi-marginal countries may become either central countries or marginal countries. The formation of the world system is based on the capitalist mode of production and the division of labor. The development of China's economy, the improvement of production methods and the improvement of the status of international division of labor have allowed China to move from a semi-marginal country to a central country.<sup>60</sup>

China's integration into the world system will inevitably lead to conflicts of interest with the United States.<sup>61</sup> As mentioned above, China and the United States are now in a state of intense competition and mutual distrust. The process of China's rise was initially based on the development of late-stage advantage and rational utilization of resource endowments. However, with the development of the economy, China's economy has also experienced many problems, such as high external dependence, weak social security system and other economic and social issues. At the same time, there are also structural contradictions in the development, such as the scarcity of high value-added products and the low level of technological innovation.

The rise of China will inevitably lead to the central position of the world system, and it is necessary to change the mode of production and its position in the international division of labor. In the current development of China, it is urgent to change the current industrial structure, strengthen the investment in scientific & technological innovation, and increase the proportion of the service industry in the industrial structure. The same as the United States, in the face of a new wave of information technology revolution, China is also eager to grasp the leading role of the next round of economic development, in order to change the mode of production and

---

<sup>59</sup> Jiang Hua: "Theory of World System: Centered on Wallerstein", Shanghai Sanlian Bookstore, 2007, p. 79.

<sup>60</sup> Elizabeth Economy & Michel Oskenberg, eds., *China Joins the World: Process and Prospects*, New York: Council On Foreign Relations Press, 2007.

<sup>61</sup> Wang Jisi: "American Hegemony and China's Rise," *foreign affairs review*, No.84, 2005.

the position of the country's division of labor, promote the sustained and stable development of the economy, promote the transformation and upgrading of the Chinese economy, and solve many problems accumulated in the process of economic development.

The issue of cyber security concerns whether China can take a dominant position in a new round of information technology change. As we mentioned earlier, cyber security affects economic development, and whether economic development affects China's status change in the world system. In the process of China's rise, one of the problems that need to be faced is the military network of the United States. China needs to develop network technology and ensure cyber security to cope with the possible network offensives of the United States and safeguard national infrastructure, national defense, and national economic system will not be in a passive position. Only when cyber security is guaranteed, can China's national interests and economic growth be maintained, and it is possible to move from the semi-marginal to the center in the world system.

In the world system, the United States is at the center. The rise of China will inevitably conflict with the interests of the United States. To maintain the central position of its world system, the United States will use cyber security as a breakthrough to limit the development of China's economy. However, there are still many points of interest between China and the United States, such as Sino-US cyber security cooperation, Sino-US trade cooperation, financial cooperation, climate cooperation, and cooperation against terrorism. These global problems are difficult to solve by the power of one country. Only China and the United States can work together with other countries in the world to find a more suitable solution to these problems. China and the United States should ensure and maintain strategic stability under the framework of dialogue and equal negotiations. This should be the key to the interests of both sides and a win-win situation.<sup>62</sup>

---

<sup>62</sup> Shen Yi: "Cognition, Competition and Cooperation in Digital Space: Cyber Security Relationship under Sino-US Strategic Relations", *Diplomatic Review*, No. 2, 2010.

## **7. Conclusion**

Nowadays, with the rapid development of information technology, the network has penetrated into various fields such as international politics, economy, military and society, and has had a profound impact on social development. Today, when globalization and informationization are mutually reinforcing, the network has been integrated into all aspects of human social life, which has greatly changed people's production methods and lifestyles. Cyber security is closely related to national security. Information technology and modernization promote each other. At the same time, cyber security shows its vulnerability, it has a great impact on many areas of a country. Cyber security has become an important part of national security. Without cyber security, there is no national security. Without informationization, there will be no modernization. Cyber security will play an increasingly important role in China's future economic development and national defense construction. Through the analysis of two cases, one is the prism gate event and the other is the ZTE Huawei event. The analysis perspectives of the two cases are different. One case uses the state as the unit of analysis to highlight the actions and strategies taken by the United States to maintain its hegemonic interests in cyber security competition. Another case is based on enterprise and enterprise backgrounds of domestic interest groups, with interest groups as the analysis unit. In order to safeguard their interests, enterprises promote interest groups to change the domestic political process and make government decisions that are beneficial to enterprises. Then, the national political and economic analysis of China-US cyber security, the network and informationization have shaped a new type of world economy. Under the background of the formation of a new world economy, the relationship between China and the United States has also undergone many changes, forming a growing situation of mistrust and fierce competition. Between China and the United States, the United States needs to maintain its hegemony in the economic field and hegemony in the political and military fields, while China is trying to rise in the world system. The two countries are competing to seize a new round of economic growth opportunities in the era of information

transformation to develop their own economies.

After making a political and economic analysis of the cyber security between China and the United States, based on the questions we proposed at the beginning, we can draw the following conclusions:

First, the production factors that dominate the economic development have changed, from capital dominant to science & technology. Cyber security is directly related to technological innovation, the quality of the institutional environment, and economic security. To achieve sustained economic growth, we must ensure continuous technological reform and innovation, a sound and stable institutional environment and economic security, and one of the foundations to ensure all of these we mentioned before is cyber security.

Secondly, cyber security issues will cause the growing distrust and fierce competition between China and the United States to continue and may worsen. The decline of the relative strength of the United States, also it tries to maintain its global hegemony status. China has experienced rapid economic growth for more than 30 years, and the economic gap with the United States has been shrinking. The US economic hegemony is the basis of its hegemony. Once the US economic hegemony falls, its political and military hegemony will also encounter different levels of challenges. In the process of safeguarding its hegemonic interests, the United States will certainly lead the next round of economic transformation with its network technology or bring difficulties to China with the offensive status of cyber security. Therefore, the game between China and the United States will be more intense because of cyber security competition.

Third, it is extremely urgent to build a new type of Sino-US network security relationship. The pattern of cyber security between China and the United States has been formed. Although the game cannot be stopped, in a world of interdependence, China and the United States must establish a network cooperation mechanism to avoid disorderly cyber struggles. That is not conducive to the economic development and social stability of any country in China and the United States, and will also affect the stability of East Asia and peace in the world.

Cyber security competition has become a big problem in challenging Sino-US relations. If it is not controlled, it is likely to seriously affect the development of Sino-US relations. Only through frank dialogue and sincere communication to eliminate misunderstandings and hostility can China and the United States seek cyber security cooperation. China and the United States should first cooperate with each other in combating cybercrime, and work together to create mutual trust, thereby alleviating the growing mutual distrust in the cyber security process between the two countries.

## 8. Bibliography

Andrew Chadwick, *Internet Politics: States, Citizen, and New Communication Technologies*, New York: Oxford University Press, 2006.

Bernstein, Richard and Ross H. Munro: "The Coming Conflict with America Foreign Affairs", March/April, 1997.

Barrientos: "Corporate Purchasing Practices in Global Production Networks: A socially Contested Terrain", *Geoforum*, 2013.

Cai Cuihong: "National Information Security Strategy of the United States", Shanghai: Xuelin Press, 2009.

Cao Jianping: "Political Economic Analysis of the International Flow of Production Factors——Based on the Perspective of Global Production Network", *International Economic and Trade Exploration*, 2013.

Collins, Randall and Michael Makowsky: "The Discovery of Society", eighth edition. Boston: McGraw Hill Higher Education, 2010.

David Scott: "The Chinese Century? The Challenge to Global Order", Hampshire: Palgrave Macmillan, 2008.

Douglas North, Lance Davis: "Theory of Institutional Change: Concepts and Causes", in Ronald Kos: "Property Rights and Institutional Change: A Collection of Property Schools and New Institutional Schools", 1991.

David Scott: "The Chinese Century"? The Challenge to Global Order, Hampshire: Palgrave Macmillan, 2008, p.157.

Elizabeth Economy & Michel Oskenberg, eds., *China Joins the World: Process and Prospects*, New York: Council On Foreign Relations Press, 2007.

Ellen Nakashima, Hacks of OPM databases compromised 22.1 million people, federal authorities say, WASH. POST, July 9, 2015,  
<https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>.

Frederic S. Pearson, J. Martin Rochester: "International Relations", 4<sup>th</sup> edition, New York: McGraw- Hill, 1998.

Freeman: "Labor Regulations and Social Protection in Developing Countries: Market Distortions or Efficient Institutions? ", NBER Working Paper No. 14789, 2009.

Frieden, Jeffrey A. , and David Lake, eds.: "International Political Economy: Perspectives on Global Power and Wealth", St. Martin's Press, 2000.

Gregory D. Grove, Seymour E. Goodman, Stephen J. Lukasik: "Cyber-attack and International Law", *Survival* no.3, 2000.

Hans J. Morgenthau: "Politics Among Nations — The Struggle for Power and Peace", Beijing: The Commercial Press Press, 1993.

Henry M.Paulson, "A Strategic Economics Engagement: Strengthening U.S-China Ties", *Foreign Affairs*, Vol.87, No.5, September/October 2008, pp.59-77.

Hu Jian, Wen Jun: "Network and National Security", Guiyang: Guizhou People's Publishing House, 2002, p.99.

Immanuel Wallerstein: "The Modern World System I : Capitalist Agriculture and the

Origins of the European World-Economy in the Sixteen Century", New Academic Press, 1994.

Jiang Hua: "Theory of World System: Centered on Wallerstein", Shanghai Sanlian Bookstore, 2007.

Jin Canrong and Dai Weilai: "Injecting Positive Energy into the Development of New Types of Great Power Relations between China and the United States - Analysis of China-US Strategic and Economic Dialogue", Journal of International Relations, No. 2, 2013.

Kenneth Lieberthal, Peter W. Singer: "Cyber security and U.S.-China Relations", February, 2012,  
<http://www.brookings.edu/research/papers/2012/01/23-cybersecurity-china-us-singer-lieberthal>.

Mark R. Amstutz: "International Conflict and Cooperation", Boston: Mc - Graw Hill, 1999.

Nicholas Westcott: "Digital Diplomacy: The Impact of the Internet on International Relations", Oxford Internet Institute, 2008.

Peter W. Singer and Kenneth Lieberthal: "Cyber security and U.S-China Relation", 21<sup>st</sup> Center Defense Initiative at Brookings, Feb.2012.

Terrence K.Hopkins and Immanuel Wallerstein, eds.,World-Systems Analysis: Theory and Methodology, Sage Publications,1982.

The White House, National Strategy to Secure Cyberspace, February 2003,  
[https://www.us-cert.gov/sites/default/files/publications/cyberspace\\_strategy.pdf](https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf).



The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009,  
[http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011,  
[http://www.whitehouse.gov/sites/default/files/rss\\_viewer/internationalstrategy\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf).

The White House, *Administration Strategy On Mitigating The Theft of U.S. Trade Secrets*, February 2013,  
[http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin\\_strategy\\_on\\_mitigating\\_the\\_theft\\_of\\_u.s.\\_trade\\_secrets.pdf](http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf).

The White House, *White House Finally Acquiesces to Congress on Cyber Deterrence Policy*, December 2015,  
<http://federalnewsradio.com/cybersecurity/2015/12/white-house-finally-acquiesces-congress-cyber-deterrence-policy/>.

US charges five Chinese military hackers cyber espionage against us corporations and a labor organization for commercial advantage, May 2014,  
<https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

U.S. Congress, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, Sept. 2016,  
<https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>.

U.S. House of Representatives 112th Congress, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, October 8, 2012.

[https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf).

Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010.

National Security Agency, Information Assurance Technical Framework, September 2002, <http://gravicom.us/downloads/docs/IATF/FtMatter.pdf>.

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cyber security, February 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

Philip Stephens, "Uncomfortable Truths for A New World of Them and US", The Financial Times, July 14, 2008.

Rid Thomas: "More Attacks, Less Violence", Journal of Strategic Studies 36, no. 1, 2013.

Rid Thomas: "Cyber war will not take place", Journal of Strategic Studies 35, no. 1, 2012.

Robert Solo: "Technology Change and Total Production Function", The Commercial Press, 1991.

Rozeta E. Shembilku: "The National Interest Tradition and the Foreign Policy of

ALBANIA”, Master of Arts in Law and Diplomacy thesis, April 23, 2004.

Shen Yi: "National Cyber Security Strategy", Beijing: Current Affairs Press, 2013.

Shen Yi: "Analysis of the Cyber Security Strategy of the Obama Administration, Modern International Relations", No. 1, 2010.

Shen Yi: "Cognition, Competition and Cooperation in Digital Space — Network Security Relationship under the Framework of Sino-US Strategic Relations", Diplomatic Review, No. 2, 2010.

Shen Yi: "Network Security and Non-traditional Factors in Sino-US Security Relations", International Forum, Vol. 12, No. 4, 2010

Sino-US cyber security cooperation is speeding up, the Ministry of National Defense of the People's Republic of China, December 17, 2015,  
[http://www.mod.gov.cn/opinion/201512/17/content\\_4632990.htm](http://www.mod.gov.cn/opinion/201512/17/content_4632990.htm).

Stephen Roach: "Can China learn from American experience? ", Economic Globalization - Asia and China, 2001.

Tikk Eneken: "Ten Rules for Cyber Security", Survival 53, no.3, 2011.

Wallerstein, Immanuel: "The Three Instances of Hegemony in the History of the Capitalist World-Economy", Social Theory: Roots and Branches edited by Peter Kivisto, Fourth Edition. New York: Oxford University Press, 2011.

Wang Jisi: "American Hegemony and China's Rise," foreign affairs review, No.84, 2005.

Wang Zhengyi: "General Theory of International Political Economy", Peking University Press, 2010.

Zalmay M. Khalizad et al., The United States and a Rising China: Strategic and Military Implications, Rand, 2006.

Zhang Shiquan: "Overall Research on National Economic Security", International Technology and Economic Research, 2003.

Zweig, David: "International China: Domestic Interest and Global Linkage", Cornell University Press, 2002.