The Origin of Security Dilemma between China and US in Cyber Space

Li Senlin*

The Institute for Social and Cultural Research, Macau University of Science and Technology, Macao Special Administrative Region Government, P. R. China.

*Corresponding Author email: senlin.li.11@alumni.ucl.ac.uk

Keywords: China and US Relationship; Cyber Security; Security Dilemma; Origin

Abstract: As the world context changed dramatically after cold war, global phenomena are being appeared continually. The cyber space, since it arose, together with land space, sea space, air space and outer space, constituted five power spaces, and naturally become a game space for nations. However, features of virtual cyber space are not same as other entities' features. Hence, this study starts with elaboration current cyber security situation faced by China and US, then, ensures what kind cyber security dilemma China and US in and reveals driving forces behind China and US cyber security dilemma. Further, the study analyses the nature of cyber space which caused cyber security dilemma in depth and offers suggestion for preventing cyber security dilemma.

1. Introduction

With the 1991 U.S. commercial Internet Exchange Association (Commercial Internet Exchange Association) announced that the Internet can be any commercial activities. The Internet will replace the determined by the U.S [1]. Department of Defense Advanced Research Projects Agency (Advanced Research Projects Agency) developed by the military network (ARPAnet) of the National Science Foundation (National Science Foundation) developed by the academic network (NSFnet) to the surface of civil network world (Internet) [2]. According to statistics, the number of Internet users worldwide has increased from 1 billion 20 million in 2005 to 3 billion 580 million in 2017, 249.6% growth in 12 years, when compared to 1997 data compared to 5014.2% growth in 20 years [3]. Under the influence of world political economy and world economic politicization, the rapidly expanding cyberspace (Cyberspace) not only continues the political and economic contradictions in the real space, but also creates new contradictions due to its unique attributes [4]. It has made China and the United States not only face the extension of cyber terrorism and other world contradictions in cyberspace, but also face the unique contradiction of network space such as network information security, and also face the real political and economic contradictions such as power distribution in cyberspace. Mapping [5].

Security Dilemma (Spiral Model) is the core concept in Structural Realism, in which both offensive realism and defensive realism are considered in an anarchic international society [6-7]. A country's consideration of its own security and its doubts about the intentions of other countries thus make the mutual improvement of military power between them is the root cause of the formation of a security dilemma [8]. Only the former emphasizes state power and the latter focuses on national security. Furthermore, neoliberalism believes that if the two sides can work out a system that can regulate the military expansion of both sides, it will not only avoid security dilemmas, but also create cooperation in an anarchic international society [9]. However, a basic means of confrontation can produce cooperation, a cooperative system is able to protect the means of production, so China in cyberspace is the collective security and security dilemma [10-12]. The collective security failed to eliminate the security dilemma between China and the US, the root of security dilemma so as to clarify the two countries in the network in the space between the two countries to help remove suspicion [13]. This article from the description of the security situation of Sino US network in space and determine whether the security dilemma in China to further clarify the cause of security dilemma

  DOI: 10.25236/erems.2018.211

between the two sides have conditions [14]. The reason further study on the above conditions of formation, and ultimately eliminate the security dilemma between the two suggestions [15].

2. Network Security Situation in China and the United States

According to the world bank, to the end of 2017, China 54 person in a hundred network. While the United States is every 64 people using the Internet, combined with the two population size, the total number of Internet users in China and the United States accounted for 28.2% of the number of Internet users in the world, and the number of Internet users is still huge room for growth China. But under prosperity with the crisis, the problem of network security is an urgent need to pay attention to, only 272 per million people in the United States Taiwan security control server (Secure Internet servers) in order to protect the security of network activity, lower than some developed countries. China has only 209 security control servers, which is less than most developing countries. The continually prosperous cyberspace continues to attract lawless people, and the fragile security system lowers the threshold for their crimes, thus sharply deteriorating the cybersecurity situation in both countries. The specific performance is:

First, the number and intensity of attacks on the underlying network and critical infrastructure has increased. In 2017, the Distributed Denial of Service continued to break new highs in the peak of China's domain name system attack traffic. Up to thousands of overseas Internet Protocol addresses have penetrated China's open industrial control equipment. And more than 30 hacker organizations attacked China's critical infrastructure network with an Advanced Persistent Threat attack. Similarly, Akama (Akamai) Company confirmed that about 75% of the internet protocol address of the target application based on virtual private network system to support the normal operation of the American public (Virtual Private System). Network security giant Kabasiji (Kaspersky) Company statistics in 2017 fourth quarter U.S. suffered a distributed denial of service attacks accounted for the global increase in the ratio of 3%, compared with the second quarter reached 16%, after China, ranked second in the world.

Second, the government and society to increase network security product demand, which is both public and private sectors, its network security spending increased year by year. In 2017, the overall size of the security market Chinese of domestic enterprises is about 43 billion 920 million yuan, an increase of about 27.6%, including cloud terminal and network edge security social security network based overall share of 70%. The same year, China industry information security market size in 2016 increased 53.6%, reaching 557 million yuan. The report pointed out that the United States in fiscal year 2019, $8 billion over budget for security, and network information system security defense. Support military command system. Maintain national security. And maintain the 133 Cyber Mission Force, and provide $95 million to secure the infrastructure network. In addition, the North American cybersecurity market is expected to grow by 10.4% annually to reach $66 billion.

In addition, the performance of network security deterioration has increased the number of hacker organizations. The disruptive activity for the data transfer process has increased. Legal provisions on network activities have increased. Increased number of cross-border cybercrime. In the final analysis, it is caused by the increasingly blurred borders of the global political economy and the open connectivity of the Internet. The network not only to promote political and economic development and hinder the development of politics and economy and then bring contradictions complex, in the Sino US security dilemma.

3. Security Dilemma and Forming Conditions of Cyberspace between China and the United States

China and the United States are facing a worsening network security situation, which gives them the impetus to form collective security. State Councilor Guo Shengqi signed the Guiding Principles for Combating Cybercrime and Related Matters in Washington on December 4, 2015 with the U.S. Attorney General and Homeland Security Secretary. In order to ensure the security and stability of

cyberspace in which the two major cyber powers coexist, the first round of law enforcement and Cybersecurity dialogue between China and the United States was successfully held in Washington in 2017 and 2018. However, in order to maintain cybersecurity, the two countries have also brought the two countries into a security predicament. The conditions for forming a security dilemma stem from the ideological contradictions of the historical relics of China and the United States, such as the differences in understanding of network terms between China and the United States. It also stems from the continuation of the power conflict between the two countries in the real world in the cyberspace, such as the competition between China and the United States for the governance of the network. It also stems from the natural contradictions between countries, such as the suspicions of the two sides on the other party's behavior. It is more due to the contradiction brought about by the attributes of the network space itself. For example, the concealment of the network makes it impossible to trace the source accurately after being attacked by itself.

However, the conditions for clarifying the cybersecurity dilemma between China and the United States must first clarify whether China and the United States are in a network dilemma and how much the judgment is: the offensive side and the defensive side have more advantages, specifically measured by network technology and network public opinion. standard. The attacking intention can be understood by the defense (Distinguishability), the specific speech acts to attack the defensive side of the dialect of the applied standards. The judgment results are as follows:

First, the United States has more offensive network technology. According to a variety of network attack map (such as: Kaspersky Cybermap) statistics show that the United States is the primary source of cyber attacks. As a founding member of America's share of the network, the root name servers (Root Name Server) is about the number of root domain server in 17%, and Chinese accounted for only 0.7%. Not only that, about 90% of current Chinese computers and mobile terminals are installed with Microsoft, Apple or Android. That is to say, the United States has implemented the overall technical control of the starting end to the terminal in the cyberspace, such as: Prism.

Second, the offensive side of the United States has more advantages in online public opinion. First of all, the United States, with its native language English as its mother tongue, combined with its developed media industry, is more able to occupy the right to speak in cyberspace. Secondly, some American network giant Google, Facebook, Amazon) over the network space in all walks of life, and its total output value is much higher than that of China network company. Finally, the so-called "American culture" in the space of network youth groups very attractive.

Third, the United States and the offensive defense Chinese can eliminate unexpected contradictions. In 1999 -2010, the two sides folk hackers to attack each other, then, in 2009 -2012 years, high-level network to ease tensions held several talks. In February 2013, Mandy company (Madiant) China accused of cyber espionage has a military background, then the two sides in 2013 years at the Annenberg estate (Sunnylands) to ease the tension. In July, the Snowden incident broke out and the two sides eased the atmosphere after the strategic security talks. In May 2014, the United States accused five Chinese soldiers of engaging in cyber espionage activities, but the two sides resolved the confrontation in a new round of strategic security dialogue. In general, the cybersecurity misunderstandings of both parties can always be properly resolved.

Based on the above judgment conditions and the Robert Jervis classification model, China and the United States are not in a high-intensity security dilemma, but there is still a problem of security dilemma. That is, the United States is the dominant party, increasing the possibility of a positive conflict, and China must develop network technology in order to ensure that it is not attacked. At this point, the relationship between the two parties may move in two directions: First, the United States still maintains its technological superiority. Once the two sides fail to develop a consensus, they fall into a double crisis (Doubly Dangerous). Secondly, China has the technological advantages and is in a controllable position, regardless of whether there is consensus on understanding between the two sides or not (Security Requirement is compatible or Doubly Safety). Therefore, China and the United States are in a low-intensity security dilemma, but what conditions make the offensive U.S. build a network security dilemma? Comparing the theoretical conditions listed by Barry R. Posen with those

created by the current security situation facing China and the United States, the following three conditions can be obtained:

First, the United States is unable to accurately assess China's network technology and strategic intentions. Every year, there are a large number of attacks against the basic networks of the two countries. In view of the concealment, non-regional and asymmetric nature of cyberspace, combined with the real world, the role of non-state actors in the cyberspace under Anarchy has been amplified. It is impossible for China and the United States to confirm whether each other is the source of the attack, whether it has some kind of attack capability, and whether it is intended to be an attack target. Therefore, the United States can only speculate on the purpose of China's network behavior based on real-world conditions.

Second, the United States mistakenly projected the hegemonic consciousness of the real world into cyberspace. The frequent occurrence of large-scale network information leakage incidents and the intrusion of important industrial control systems will inevitably make the two countries realize that the anarchy of cyberspace is far stronger than the anarchy of the real world. Therefore, the relative control of cyberspace is the inevitable result of two big countries. The United States intends to establish control over the entire cyberspace hegemony, even if other countries obey the network rules it has established. However, controlling the control of the entire cyberspace is bound to infringe on national cyber sovereignty. Therefore, in Russia and other countries to the United Nations in 2011 submitted to the "international code of conduct for information security" proposal, emphasizing national sovereignty and the rule that network network space should be borne by the United Nations in respect their wishes and establish conditions.

Third, the United States is still the ideology as to build their own network security according to the. The essence of the Internet is neutral, but in the network so that it is no longer a neutral country. The United States several times in the network space to government and non government role Chinese false discussion of human rights and democracy and other issues, and then create Chinese to steal the property of military, business, and other network information network role. Furthermore, restrictions and sanctions are imposed on Chinese outstanding companies to enter and develop the US market (such as ZTE, Huawei, etc.) and to monitor Chinese American experts. Both of them make China and the United States unnaturally form a confrontation in cyberspace to maintain the virtual image of the United States leading unilateral network affairs.

4. Roots of a security dilemma

The conditions for forming a network security dilemma are not the castles in the air, but the environment of the two countries, which is caused by the natural characteristics of the network space. As the battlefield environment strategic behavior. Therefore, the security dilemma between China and the United States conditions formed in cyberspace must be affected by the nature of the network space itself. In the final analysis, the following three points derived from the form of security dilemma conditions:

First, the network space (Anarchism). The network space between countries will fuzzy boundaries. The scope of a country can only support based on the network of sovereignty. Therefore, cyberspace does not have a world government that is above the national government, but there are non-state behaviors in the jurisdiction far more than the real world and the space for many individuals or organizations. Therefore, the United States is more eager to manage and hegemonize cyberspace.

Second, there is a complex relationship between cyberspace and the real world. Even though the network makes the country's Asymmetry in cyberspace more obvious, cyberspace continues the relationship between countries in the real world. First, it continues the contradictions between China and the United States in the real world (such as trade, rulemaking, etc.), so that the two countries continue to wrestle in the cyberspace. Secondly, it continues the illegal activities in the real world (such as terrorism) and makes the two countries have the goal of cooperation. Finally, it also continues the basic attributes of Great Power (e.g. the pursuit of security), thus enabling the two countries to naturally pursue comparative network advantages.

Thirdly, cyberspace relies on Substance. Without the basic material as the basis (such as chips, cables, etc.), network space will no longer exist. Therefore, countries will consciously improve their ability to produce network equipment and the performance of network equipment. Which country has the dominant technology will occupy the dominant position of cyberspace. Therefore, even if China and the United States are in a situation without threats, they will actively pursue better network technology, thus forming a coincident security dilemma. This not only has the role of big country attributes, but also the internal driving force in the network industry.

5. Suggestions to China and the United States

To sum up, the countermeasures to eliminate or alleviate the security dilemma in the Sino-US network must take the nature of cyberspace as the basic starting point, that is, must understand the advantages and disadvantages of the nature of cyberspace. Therefore, countermeasures against the adverse aspects of the nature of cyberspace should be taken to eliminate its adverse effects as much as possible. At the same time, unfavorable and favorable surface downside favorable surface to understand the nature of the inside, combined with the natural attributes of the two powers, and thus to be rational and based recommendations, summarized are the following three points:

First, the concealment does not mean that the network no responsibility network space. Network space hidden features that make people and organizations and the country may engage in activities and play without any constraints. This characteristic heightened the trust relationship between countries, thus, the network must be the responsibility, right and freedom is the responsibility of the network activity is not occupied, but the responsible for their own words and deeds. Therefore, both parties should establish and improve their own network laws and network supervision systems. The network supervision system is not a violation of civil rights, it is precisely to protect the security of citizens' information and property.

Second, the non-regional nature of cyberspace does not imply the non-regional nature of state management. The non-regional, holistic and complex nature of cyberspace has blurred the boundaries of the real world. In turn, the world is highly integrated and the world economy is driven. But it also makes crimes, terrorism and other acts worldwide. In view of the fact that there is no world government beyond the national level, it is essential for China and the United States to control the domain under their control to ensure the cleanliness of cyberspace. Therefore, China and the United States should actively and properly establish a network security maintenance mechanism and assume the responsibility of network security protection after clarifying the legal provisions of their own network domains.

Thirdly, the cultural nature of cyberspace does not mean that the network is the battlefield of the conflict between soft power and civilization. The diversity of cyberspace guarantees the continuous renovation and change of the world cyberculture, and also makes the staggered progress of design, creation, academia and other fields in the real world. But cultural interaction brings not only the help of progress, but also the resistance of conservatism. However, a country should not use resistance as an excuse to confront other countries, nor should it regard the "zero casualties" cyberspace as a battlefield for "civilization." Therefore, China and the United States should strengthen multi-level exchanges and cooperation, and promote social cooperation in various fields such as art, ideology, culture, and science and technology through social forces.

References

[1] Cavelty M D. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities [J]. Science & Engineering Ethics, 2014, 20(3):701-715.

[2] Popa I F. Extensive Transparency as a Principle of Cyberspace Governance and Cyber Security Dilemma Prevention [J]. Social Science Electronic Publishing, 2015:59-62.

[3] Alexseev M A, Hofstetter C R. Russia, China, and the Immigration Security Dilemma [J].

Political Science Quarterly, 2013, 121(1):1-32.

[4] Scobell A. Strategic Reassurance and Resolve: U.S.–China Relations in the Twenty-First Century by James Steinberg and Michael E. O'Hanlon. Princeton, NJ, Princeton University Press, 2014. 272 pp. $29.95.[J]. Political Science Quarterly, 2015, 130(3):546–547.

[5] Zachary C, Igor L, James L. Four domains of cybersecurity: a risk-based systems approach to cyber decisions [J]. Environment Systems & Decisions, 2013, 33(4):469-470.

[6] Rosoff H, Cui J, John R S. Heuristics and biases in cyber security dilemmas [J]. Environment Systems & Decisions, 2013, 33(4):517-529.

[7] Alexseev M A. Societal security, the security dilemma, and extreme anti-migrant hostility in Russia [J]. Journal of Peace Research, 2011, 48(4):509-523.

[8] Aissa A B, Abercrombie R K, Sheldon F T, et al. Defining and computing a value based cyber-security measure [J]. Information Systems and e-Business Management, 2012, 10(4):433-453.

[9] Zhang M. Time to Change the Truancy Laws? Compulsory Education: Its Origin and Modern Dilemma [J]. Pastoral Care in Education, 2004, 22(2):27-33.

[10] Malkin L, Elizur Y. The Dilemma of Dirty Money.[J]. World Policy Journal, 2001, 18(1):13-23.

[11] Smith S P. between Pozzo and Godot: Existence as Dilemma [J]. The French Review, 1974, 47(5):889-903.

[12] Takahashi S, Liang L. Roles of forests in food security based on case studies in Yunnan, China [J]. International Forestry Review, 2016, 18(1):123-132.

[13] Hooper K. Alternative Genealogies? History and the Dilemma of "Origin" in Two Recent Novels by Galician Women [J]. Arizona Journal of Hispanic Cultural Studies, 2006, 10(1):45-58.

[14] Albert J,, Adamek H E, Weitz M,, et al. [Pancreatic duct stenosis of uncertain origin. A case of diagnostic dilemma][J]. Internist, 2002, 43(2):263-267.

[15] T Böttger. [Pancreatic tumor of uncertain origin--a therapeutic dilemma?][J]. Langenbecks Arch Chir Suppl Kongressbd, 1998, 115:1123-1126.