Research on Cyber Space Security Strategy of the United States

Tianming HUANG
College of Arts and law, Wuhan Donghu University, P.R.China,
51124385@qq.com

Abstract Into the 21st century, information revolution speed up development, unprecedented advance of globalization, cyberspace has become a human life, production, and war is highly dependent on the "fifth space", the network space safety aroused wide attention from all over the world. The us cyber space security strategy has experienced three stages of development, namely "comprehensive defense, protection of facilities" -- "combination of attack and defense, cyber counter-terrorism" -- "focus on attack, and network deterrence". The cyberspace security strategy suggests that the development of a country to be able to well against cyber threats, it is necessary to strengthen their own web space deterrence, only is mindful of its own strength, to occupy the initiative in the international network space game.

Key words Cyber space; Security; Strategy

1 Introduction

In today's society, with the extensive application of information technology, "cyber space" is gradually becoming a special field covering social, political, economic, cultural and military activities. The emergence of cyber space has effectively promoted the progress of political multi-polarization, economic globalization and social informatization, and brought new vitality to the development of the whole world. But at the same time, network space safety incidents occur frequently in recent years is also a wake-up call for us, more and more countries begin to develop security in cyberspace, cyberspace has become the land, sea, air, since the day of the fifth big security domain.

2 The Situation of Network Space Security

2.1 The development of cyberspace has changed the trend of world development

Famous American futurist alvin toffler predicted that in the 1980 s and the network electronic technology will lead a new civilization appear in our life, it will change our original thinking mode, bring us a new way of life, and lead us into a new economic and social. [1] now we can see that toffler's prophecies are being fulfilled one by one. In just a few decades, the Internet constantly improve, many countries compete to build information network infrastructure, global network users reached 2 billion, all kinds of wireless digital equipment more than 4 billion units, the network space is gradually become the basic and crucial influence the world development, strategic significant emerging field. Network space itself is made of the information network and the information carried by the global information environment, it is by changing the information behavior of human society greatly influenced the modern world the development of economy, politics, culture and military. At the economic level, with the close combination of network and globalization, network space promotes economic globalization to evolve in depth. At the political level, the continuous expansion of network space and the increasing expansion of network society have led to the decentralization of political power to a certain extent. At the cultural level, Internet space, as a global platform for cultural interaction, has greatly promoted the exchange and integration of the world's ideology and culture. In military terms, the emergence of network space, will directly lead to the mechanized war era platform centered mode and operational forms for army to adapt to modern warfare network-centric mode and operational forms for army, cyberspace as a direct carrier of the information technology, through the interaction with land, sea, air, day, enlarged the scope of the battlefield, fuzzy boundaries discussed, directly to accelerate the process of the history of the world new military revolution.

2.2 Competition in cyberspace leads to international strategic games

In recent years, along with the rapid development of network space, countries around the world are also increasingly fierce competition for space network control, just as toffler predicted, who mastered the information, control of the network, who will have the entire world. The United States, as the birthplace of the Internet, is the first country to wake up, first act and first benefit in the field of cyber space. as early as in 1993, the Clinton administration first proposed "the national information infrastructure", after twenty years, the U.S. government has issued "information security technology framework", "national security strategy report", "the information system to protect national plan", "national network space safety strategy", "national security strategy report", journal of the American academy of cyberspace policy review, "idea of network in the United States army combat ability", "national security strategy report", "American network space international strategy" and "American network space action strategy" and so on ten strategic documents, We have basically completed the top-level design and overall planning for the construction and development of national cyber space power, and formed a complete national cyber space strategy system. Russia openly carried out as early as 1995, the information, information and network protection act, after Mr Putin came to power, to further speed up the development of the field of network space, in March 2002 by the "2010 and the future Russian basic development policy in the field of science and technology in the information technology as one of the nine science and technology development priorities. In 2005 the development of national information and communication technology infrastructure federal special plan ", aimed at developing residents Internet infrastructure construction, improve the degree of social informatization, it is easy to find from the war with Georgia, Russia has use of network space against the hostile forces of military power. To remove these two super military powers, Germany and France, respectively in 2005 and 2008 and issued a "information infrastructure protection plan" and "network defense and national security" special reports, the British introduced in June 2009 the first "national cyber security strategy", Japan, South Korea, India and other countries have also introduced a cyberspace related strategy document, Iran, north Korea, Israel and other countries also have begun to use the web space in the local conflicts to achieve strategic goals.

2.3 Cyber space threats pose new security challenges

Real-time, openness and tolerance of the network space determines the existence of great safety hidden trouble, especially along with the advancement of information globalization, any organization or individual has a chance to through cyberspace loopholes and defects of the hostile forces attacked, once these attacks may space through the network to ten million times the size of the burst, causing catastrophic. There is no doubt that China, with the largest number of Internet users in the world, is a cyber power, but not a cyber power. According to the 2013 cyber attack report statistics, the source of malicious attacks, malicious codes, Web attacks, phishing hosts and botnets are all from the United States. According to the latest ranking of countries with cyber defense capability by us technology information website, China ranks low, far behind developed countries such as Europe, the us and Japan. Because China's lack of the core technologies in the field of network space, a personal computer and the operating system of intelligent terminal comes from the United States and other developed countries, China is not set against the basic network attack. In addition, of the 13 root Internet server in the whole world, the United States has already mastered one of the ten, but none in China, the root server is the interpretation of the domain name in the end, the best server, national body can control the root server to take control of the Internet. [5] at the same time, as more and more countries began to military power in the network space development, network space as the basis of information war, in the military strategy has unshakable center position.

3 Development of the US cyber space security strategy

3.1 Comprehensive defense and protection of facilities

The United States is not only the first country in the world to popularize the Internet, but also the first country in the world to study the cyber space security strategy. The Clinton administration recognized the importance of cybersecurity in the United States as early as 1993, and officially adopted the concept of "information security" for the first time in a 1998 government report. The U.S. government will recognize the early, along with the wide application of network information technology, the social networking trend is inevitable, and the intrinsic characteristics of cyberspace decided we cannot completely eradicate the loopholes and defects, the objective existence of cyberspace threat, are on the critical national infrastructure and material assets pose a serious security hidden danger. For all these reasons, the nsa has developed the information technology security framework (IATF) based on the cybersecurity framework. The IATF initially divided security solutions into four 'Defense in Depth' focus areas to deal with potential cyber attacks on infrastructure. As the U.S. government to deepening understanding of the cyber space, IATF has also undergone multiple versions of the revision, published in September 2002, the latest IATF3.1 version) in the (IATF4.0 is compiling, further expansion of the scope of "defense in depth", many civil network security. As the core of the whole IATF, defense in depth strategy using a multi-level, deep security measures to protect the security of user information and information system, people, technology and operation as the strategy of three core factors, is the important foundation of information security, the lack of any one of them will be great influence to the whole strategy implementation. With the continuous promotion of this application, the content and ideas contained in IATF have been widely used in the information.

3.2 Combination of attack and defense and Internet counter-terrorism

The outbreak of the September 11 terrorist attacks led to a sharp change in the us government's attitude towards cyber space security, which directly led to a change in the us national cyber security policy choices. With the rapid rise in demand for network space security, the U.S. government for the construction, expansion, great chance to improve network security strategic function, under the leadership of President George w. bush administration to respond quickly, enacted a series aimed at strengthening the network security policies and regulations of the construction of the space.

During the bush administration, America's cyber space security strategy gradually changed from defense to attack. Compared with the Clinton administration, the bush administration put forward "critical infrastructure" is not only to protect their own information security mechanism, are also trying to to foreign countries to monitor network security infrastructure, this undoubtedly reveal a strong offensive. In addition, the period of the us government pay more attention to developing foreign intelligence gathering capability, information capability and network capability, including "Einstein project", "comprehensive information perception system", "prism" and so on a number of network intelligence monitoring plan during this period. Published in 2002, the U.S. national security strategy report clearly put forward to develop the remote sensing, long distance precision strike capability, can change the military power, and information warfare capability is one of the important link. At the same time, the United States plans to influence the ideology of less developed countries in Asia, Africa and Latin America, including China, through cyber diplomacy to serve its national interests.

3.3 Focus on attack and cyber deterrence

The beginning of Mr Obama took office, led by the us government has released the U.S. cyberspace policy review report, the report assessed the cyber security strategy of the United States, points out the existing problems, put forward a plan of action. In the report, the concept of "cyberspace" was reaffirmed, the status of cyber space as the main battlefield was further emphasized, and the "cyber threat theory" was promoted. In May 2011, the Obama administration released the international strategy for cyberspace. In the report clearly pointed out that cyberspace has become a important strategic base for the future development of the United States, the U.S. government will maintain the current American advocate freedom as much as possible of cyberspace security pattern, ensure the safety of the American Internet controls, to ensure that U.S. interests expand international cooperation, said it would mobilize the political, economic, military, diplomatic, all means such as technology and resources to ensure that the network security and development space. In July 2011, the us defense department released the us cyber space action strategy, a military interpretation of cyber space security strategy. Report based on the analysis of the strategic environment and network threats, respectively from the operational concept, defensive strategy, the domestic cooperation, international union and talent training and five aspects of technical innovation initiative. report made clear a period in the future the development direction of U.S. cyberspace operations, planning the strategic roadmap, clearly highlight the American tried to dominate the world network through strategic planning formulated the strategic vision of development.

In April 2015, the U.S. defense department released the latest action strategy for the network space, it is considered to be guiding power network defense development, strengthen the network defense, realize network deterrence guidance documents. [12] in the document, three key points of current us cyber security facilities and five targets of the pentagon's cyber space force in the next five years are highlighted. The document publicly confirms that the us military can carry out cyber attacks in the face of so-called threats, and clearly lists the countries it believes are most at risk: China, Russia, Iran and north Korea.

4 The enlightenment of the us cyber space security strategy to China

The cyberspace security strategy suggests that the development of a country to be able to well against cyber threats, it is necessary to strengthen their own web space deterrence, only is mindful of its own strength, to occupy the initiative in the international network space game.

4.1 Formulate cyber space security strategies in line with China's national conditions

Cyber space security strategy is the specific policy basis to guide the country to deal with cyber space security threats and to develop cyber space security capability. Issued from the world's major countries over the years we can see that in network space safety strategy effective cyber security strategy should include the following several parts: the first thing to make objective analysis about the present situation of domestic cyber security, state security in cyberspace facing the opportunities and challenges. Secondly, the main strategic goals of the development of cyberspace should be put forward according to the actual situation of the country. Thirdly, it is necessary to formulate specific development plans for the realization of strategic goals in cyberspace, and formulate corresponding implementation plans and countermeasures according to the plans.

Along with the rapid development of space technology, the network of a country in different period need network space safety problems will be different, and cyberspace security strategy also needs accordingly. In America, for example, in a short span of 20 years, along with the unceasing change of domestic network space safety situation, the cyberspace security strategy has experienced from the defensive to the offensive and defensive based deterrent to network three development stages, in each stage of the proposed strategic targets are different. In fact, in view of the increasingly complex situation of international cyber space security, the United States has made adjustments and improvements to its cyber space security strategy in recent years. The practical experience of the United States that, at the top of complete design is necessary for the construction of the security forces in cyberspace, formulates conforms to the situation of network security strategy space, on the one hand, can for their own network space construction of security forces have a clear aim, and formulate the corresponding development plan, put forward the corresponding construction requirements; On the other hand, it can also clarify the responsibilities of various departments in the process of maintaining the security of network space, so as to improve the efficiency of the use of network space power.

4.2 To coordinate the rapid and coordinated development of cyber space security forces

With the international security situation of network space is increasingly severe, the importance of the construction of the security forces to cyberspace is also rising, given the close link between cyberspace and other security space, must be in the process of construction of the security forces in cyberspace attention as a whole of cyberspace security forces and other security forces rapid coordinated development.

For a country to coordinate and rapid development of cyberspace security forces as a whole, on the one hand, should be from institutions, equipment research and development, talent reserves, application practice multiple links such as strengthening the construction of cyberspace security forces in an all-round way. Specific view, should set up specialized network space safety management and coordination agency as soon as possible, and identify each other departments at all levels in the network space protection responsibility, should be constantly to improve overall qualities of cyberspace security professional team gradually expand the scale at the same time, further speed up the cutting-edge network space safety equipment research and development and the update frequency, continuously broaden the sources of cyberspace security personnel channels, increase the quantity of network information of special talent reserves, pay attention to network security forces in the field of space application practice, upgrading network space threat protection departments at all levels for efficiency. Must be combined with the network space, on the other hand, the "land, sea, air, day" and other wide in the field of security, clear cyberspace security forces and the other the relationship between the security forces in the field, in the process of construction of the security forces in cyberspace mutual fusion, to promote the security forces in the field of the whole country the rapid coordination development of the security forces.

4.3 Enhance the overall strength of cyberspace through military and civilian integration

In network space process of the construction of the security forces in the United States, we can see not only the government and the army of mutual cooperation, at the same time can also see the army with the close linkage between local businesses and individuals. To organize the implementation of network warfare exercises in recent years in the United States, from the private sector in the unit continues to increase, publishes the communication between the increasingly frequent, most of the network space weapons and equipment are made by the military and private enterprise to develop, the cost savings at the same time also makes the r&d efficiency is improved. In response to the threat of cyberspace in the process of implementation of civil-military integration strategy, need to move flexibly interactive development of cyberspace security industry fusion, flexibly to achieve complementary advantages between enterprises, speed up the national independent controlled the development of information technology; It is necessary to strengthen the exchange and cooperation of high-tech talents in military cyberspace and realize the common use of high-tech talents in cyber space. In fact, with the continuous narrowing of the gap in cyber space technology between the military and the ground, military and civilian integration has become an important strategy to enhance the overall strength of the country's cyber space.

References

[1] Liu Qingsong, Wang Dan. A review of the new development of American cyber space policy from the assessment of cyber space policy [J]. Journal of the armed police command institute, 2013 (3):18-21.

[11] Xiao Lin, Yang geng. Brief analysis of the content of the defense department's cyber space strategy [J]. Journal of the air force command institute, 2014 (2):34-40.

[12] Liang Meng, Han Yue, Qiao Zheng. Review of the us department of defense's cyber space strategy [J]. Defense technology, 2015 (1):68-72.

[13] Chen Zhike, Xiong Wei. Research on the development of American network space [J]. Journal of equipment institute, 2017 (2):89-93.