DOI 10.15302/J-SSCAE-2016.06.016

Emergency and Response for Cyberspace Security

Yu Quan[1], Yang Lifeng[2], Gao Guijun[2], Kou Ziming[2], Zhai Lidong[3]

1. Institute of China Electronic Equipment System Engineering Corporation, Beijing 100141, China
2. Taiyuan University of Technology, Taiyuan 030024, China
3. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China

Abstract: Based on the current situation and main problems of cyberspace security in China, this paper proposes that cyberspace security should shift its focus from an emergency-based approach to a response-based approach. Some transformation strategies are proposed, including three aspects: cyberspace security monitoring capacity, cyberspace security guarantee capacity, and talent construction capacity.

Keywords: cyberspace security; emergency for cyberspace security; response for cyberspace security; transformation strategy

1 Introduction

In recent years, China's influence in cyberspace has gradually increased. In January 2016, the China Internet Network Information Center (CNNIC) released the 38th Statistical Report on Internet Development in China. As of June 2016, the number of Internet users in China reached 710 million, and the penetration rate reached 51.7%. This exceeded the global average of 3.1%, and was more than 8.1% above the Asian average. The total number of domain names with the China country code ".cn" is 16.36 million. This number has exceeded the number of German national top-level domain names using ".de." China's ".cn" domain names have achieved the top-most national and regional levels along with the world's first registered ownership. Mobile Internet has created a new form of social life. "Internet Plus" action plans continue to help the development of enterprises. The impact of the Internet on society as a whole has entered a new stage [1].

However, China's cyberspace security is still facing a very serious threat. On the one hand, the international situation of cyberspace security is complex; the United States, Europe, and other developed countries are strengthening the deployment of cyberspace, thus increasing the risk of an arms race in the global cyberspace. In addition, cross-border cyber attacks and cybercrimes occur frequently, and the global large-scale cyber conflict risk is significant. On the other hand, China's cyber attacks and defenses, cyberspace security industry as well as the construction of cyberspace security laws and regulations and cyberspace security personnel team have made considerable progress. However, the overall ability to protect China's cyberspace security still needs to be improved. China's legal system, mechanism, and related measures for China's cyberspace security also need to be improved [2].

China's President Xi Jinping made it clear that "if there is no cyberspace security, there will be no national security," and "without informatization, there will be no modernization [3]". Cyberspace security has become a critical part of the overall framework of the national security concept. Therefore, ensuring cyberspace security in China and scientifically responding to cyberspace security incidents are greatly significant.

Cyberspace security emergency and its response are two types of reactions to cyberspace security incidents. An emergency-based approach is an unplanned activity that occurs during cyberspace security incidents and is a passive approach. In con-

Received date: 8 October 2016; **revised date:**18 October 2016
Corresponding author: Yu Quan, Chinese Academy of Engineering, Academician; Institute of China Electronic Equipment System Engineering Corporation, Researcher. Major research fields include software-defined radio, mobile Ad hoc network, cognitive radio network, next-generation wireless communication network, spatial information network, etc. E-mail: yuquan61@qq.com
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 079–082
Cited item: Yu Quan et al. Emergency and Response for Cyberspace Security. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.016

trast, a response-based approach to cyberspace security incidents requires targeted and planned activities, determines the scientific reason for cyberspace security incidents that have occurred or may occur, and is an active approach.

We have fully realized that to ensure China's cyberspace security, we cannot rely only on the passive emergency-based approach after an incident but must have a scientific and positive response-based approach. A process is needed to achieve this transformation.

2 Improve the monitoring ability of cyberspace security to ensure the transition from emergency to response

The three stages of the development of cyberspace security incidents are as follows: in advance, during the incident, and after the incident. An emergency-based approach implies treatment of the situation after an incident, while a response-based approach implies controlling the matter when it occurs or even in advance. "Preparedness ensures success and unpreparedness spells failure." If we can do a good job of prevention and early warning in advance, we can effectively deal with occurrences of cyberspace security incidents. It is very important to find minute and unsafe factors in time, and use various advanced techniques and methods to strengthen the monitoring capability of cyberspace security.

2.1 Network monitoring scope should be more extensive and complete

What is the protection objective of cyberspace security? This is the first issue to be determined in network monitoring. Academician Fang Binxing pointed out the boundary of cyberspace security: Cyberspace security involves electromagnetic equipment, electronic information systems, operation data, and security problems in the cyberspace. It is necessary to prevent, protect, and dispose problems within the Internet, telecommunication networks, radio and television networks, Internet of Things, computer networks, online social networks, computing systems, communication systems, control systems, and other information communication technology systems, and to ensure that the bearing data is not compromised. We must also prevent the abuse of information communication technology systems with regard to political, economic, cultural, social, and national securities. To prevent these risks, we should adopt a comprehensive means of law, management, technology, and self-discipline to cope with and ensure confidentiality, availability, and controllability [4].

2.2 Network monitoring scope of business should be expanded

With the expansion of cyberspace, many security incidents have occurred in various fields, including mobile application (APP). Network monitoring should be as extensive as possible to cover all existing businesses, and not only to monitor conventional businesses. A business should be upgraded and expanded in surface and abstract states to accurately analyze what is meant to be monitored.

2.3 The granularity of network monitoring should be increased

We need full-flow monitoring because the original network monitoring only focused on traffic, resulting in many abnormal incidents being ignored. We need to conduct not only full-flow monitoring but also data element extraction and focused monitoring of the key link to cover more information. When the amount of information increases, we can use big data to conduct an in-depth study, obtain a meaningful objective impression, and use these objective impressions to guide the important aspects of cyberspace security monitoring.

2.4 Network monitoring links should be made a distinction between the primary and the secondary one

From the viewpoint of a network structure, the network monitoring links generally include Internet users as the outermost end and Internet data center (IDC) as the middle link. The innermost end is the backbone network. When monitoring the network, we must clarify as to which of these links can be combined, what are the links that should be focused upon, and the weights of these links. Usually, the backbone network has the strongest protection capability and extends outward to all links at the end. The protection capability of a network structure is multidimensional and cannot be monitored according to a unified standard. It should be monitored in terms of primary and secondary links.

3 Enhance the overall safeguarding capabilities of the cyberspace security to achieve a transition from emergency to response

Many factors restrict improvements to the overall security of cyberspace in China. For example, China's cyberspace-security-related legal system, mechanism, and institutions are still relatively backward in comparison with those of the United States, Europe, and other developed countries. The problems include lack of excellent cyberspace security personnel, lack of offensive and defensive capabilities for cyberspace security, and the relative weakness of the basis of the domestic cyberspace security industry. To achieve change, we need to fundamentally change the current cyberspace security situation.

3.1 Strengthen the emergency linkage of cyberspace security

Large-scale emergency linkage is the most effective method to improve the emergency and response of cyberspace security incidents and the safeguarding capabilities of cyberspace security.

However, the cyberspace security emergency system in China lacks a unified top-level leadership, and emergency management is assigned to different departments according to different network content and properties. Emergency organizations at all levels have geographical restrictions, which are inconsistent with the geographical independence of the Internet.

For a passive emergency-based approach to cyberspace security incidents, the emergency entities lack an effective method of cooperation owing to administrative planning and other reasons. Thus, China should conduct a top-level redesign of cyberspace security management as soon as possible, and establish an emergency response center for the central leadership of cyberspace security. China should also establish a linkage mechanism for emergency response between different departments and networks. The integration of emergency management functions of cyberspace security scattered across different business sectors will enhance the efficiency of emergency response [5]. To further strengthen the emergency linkage of cyberspace security, China should establish an efficient information and resource sharing mechanisms for cyberspace security emergency as soon as possible. Thus, the ability to assess cyberspace security situation could be improved, and could provide adequate warnings, decision making, and reaction time for cyber space security emergency.

3.2 Clear cyberspace security emergency responsibility

For a long time, the problem of cross-departmental supervision has plagued China's cyberspace security management. The clarification of the responsibility for cyberspace security emergency in the form of law is an important part of enhancing China's overall cyberspace security. The legal boundaries of Internet-content management and technology management should also be well-defined. In addition, it is important to establish clear responsibilities, rights, and status of the cyberspace security management departments when facing a cyberspace security emergency, determine law enforcement departments, and improve the coordination mechanism [6].

3.3 Deepen international cooperation in cyberspace security incidents

Under the new situation of globalization of current Internet governance, especially since the "PRISM-gate" incident, all the countries worldwide are actively striving for the dominant right of the network. The development of international rules and regulations for cyberspace and behavior norms is an increasingly urgent need. China should expand international discourse of cyberspace from the legislative viewpoint of China's "cyber sovereignty," thus strengthening international cooperation to examine cyberspace security incidents. This is very important in enhancing the overall ability to protect the cyberspace security.

First, China should establish "respect of cyber sovereignty and maintaining cyberspace security" as its premise, and promote the establishment of a multilateral, democratic, and transparent international Internet governance system. The formulation of international rules in cyberspace is important in combating cross-border cybercrime, and deepening international cooperation in cross-border data flows and other fields. Second, China must ally the International Telecommunications Union (ITU) and other international organizations to strengthen international cyberspace security consultation and dialogue, and expand the international influence and discourse power of cyberspace. Third, China can encourage and guide domestic enterprises, academic, and research institutes to actively participate in international exchange and research of cyberspace security. This will improve the new order of global cyberspace.

3.4 Establish a cyberspace security emergency standard system

According to the Information Security Technology: Guidelines for the Category and Classification of Information Security Incidents (GB/Z 20986–2007), China's cyberspace security and information security incidents can be divided into four levels [7]. However, because the existing classification of the damage degree and influence scope is broad, it is difficult to translate into a specific, quantifiable economic operation, and social stability evaluation index. This leads to the timely warning or classification of cyberspace security incidents, affecting the effective implement of response operations. Therefore, the establishment of the framework for a cyberspace security emergency standard system, including cyberspace security emergency management standards, technical standards, and service standards, is very important. This will perfect a cyberspace security emergency standard system, especially with network emergency monitoring, early warning, and disposal standards as well as contingency plan systems.

4 Strengthen the construction of cyberspace security talent team to speed up the transition from emergency to response

From the talent perspective, because an emergency-based approach has no sufficient advance warning or preparedness, cyberspace security incidents tend to occur. To eliminate the impact of an incident as soon as possible, the requirements in all aspects for the personnel to handle cyberspace security incidents are relatively high, while responses need minimum requirements for the personnel to deal with emergencies because of sufficient preparedness and an appropriate response scheme.

With the increase in the complexity of the cyberspace security situation, the shortcomings of cyberspace security talents in China have been revealed. For example, there is a supply-and-demand imbalance with regard to our cyberspace security talents: The supply is far less than needed. In particular,

China lacks a high level of leading talents. Unsound incentive mechanisms lead to the brain drain, and this even leads to hacking or cybercrime. Therefore, response to cyberspace security incidents should be people-oriented and speed up the training of cyberspace security talents.

4.1 Cyberspace security talent system planning

The top-level design of cyberspace security talent training should be accelerated. In addition, China should design the cyberspace security talent system planning. This is of great significance to ensure the continuity of cyberspace security talents and the independent innovation of core technologies. In June 2015, China officially classified "cyberspace security" as a first-level discipline [8]. It is very important in determining the overall deployment of talent training, developing talent training programs, adjusting structural programs, and optimizing resource allocations.

4.2 Improve the cyberspace security talent training mechanism

Cyberspace security talent training should be based on general higher education. Furthermore, vocational higher education and social training should play a supporting role. Owing to the rapid updating of industry knowledge and the high complexity of problems faced, it is necessary to address the issue about the continuing education problems of cyberspace security practitioners. To perfect cyberspace security talent training mechanisms, universities, research institutes, and enterprises can try to open attack-defense platforms and national cyber range through market-oriented mode, strengthening the cultivation of cyberspace security professionals and compound talents. At the same time, it is necessary to establish a relevant talent assessment and incentive mechanism and fully mobilize the enthusiasm and initiative of culturists and trainees.

4.3 Promote leading talent training in the field of cyberspace security

China's President Xi Jinping suggested the emancipation of the mind and cherishing of talents. Special talents should be treated with special policies [9]. In the cyberspace security field, special funds should be implemented for special talents; a special assessment and payment system should be established for leading talents; a major research plan should be developed, and young academic leaders should be cultivated selectively, thereby introducing and cultivating cyberspace security leading talents. In addition, China should build a number of key innovative teams with different major directions of cyberspace security in scientific research institutes with relative advantages to form a batch of training bases for high-level talents.

5 Conclusions

Absolute security does not exist. The basic properties of the Internet include collaboration and sharing. If these properties are lost, then the cyberspace security is of no significance. Therefore, it is necessary to strengthen strategic research of cyberspace security, enhance the monitoring capabilities of cyberspace security, improve the overall safeguarding capabilities of cyberspace security, and accelerate the construction of a cyberspace security talent team. These issues are very important in transitioning cyberspace security from a passive emergency response to an active one and from conventional experience-based emergency response to modern technology-based one. This also has a high significance for China to generally improve its national security capability in a turning to a cyber power.

References

[1] China Internet Network Information Center (CNNIC). The 37th statistical report on Internet development in China [EB/OL]. (2016-01-22) [2016-10-08]. http://www.cac.gov.cn/2016-01/22/c_1117858695.htm. Chinese.

[2] National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). 2015 China Internet cybersecurity situation summary [EB/OL]. (2016-04-22) [2016-10-08]. http://www.cert.org.cn/publish/main/12/2016/2016042208505 6915532001/20160422085056915532001_.html. Chinese.

[3] News of the Communist Party of China. Xi Jinping's view of the network: No cybersecurity, no national security [EB/OL]. (2014-11-20) [2016-10-08]. http://cpc.people.com.cn/xuexi/n/2014/1120/c385475-26061137.html. Chinese.

[4] Fang B X. Cyberspace security includes four levels of security [EB/OL]. (2015-12-16) [2016-10-08]. http://tech.qq.com/a/20151216/051549.htm. Chinese.

[5] Feng T, Zhang Y Q, Cao Y X. Network security incident response linkage system model [J]. Computer Engineering, 2004, 30 (13): 101–103. Chinese.

[6] Sun Y H. Ten problems and legislative strategy of China's cybersecurity [J]. China Information Security, 2014, (10): 40–43. Chinese.

[7] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Information security technology—Guidelines for the category and classification of information security incidents. GB/Z 20986–2007 [S]. Beijing: Chinese Standards, 2007. Chinese.

[8] The Academic Degrees Committee of the State Council, the Ministry of Education. Notice on setting up the first level discipline of cyber space security. Degree [2015] No.11 [Z]. Beijing, 2015. Chinese.

[9] Xinhua News Agency. The speech of Xi Jinping on the cybersecurity and information work conference [EB/OL]. (2016-04-25) [2016-10-08]. http://www.cac.gov.cn/2016-04/25/c_1118731366.htm. Chinese.