DOI 10.15302/J-SSCAE-2016.04.006

Study on the Development of China's Cyberspace Security Industry

An Da, Liang Zhihao, Xu Shouren

China Academy of Electronics and Information Technology, Beijing 100041, China

Abstract: This paper summarizes the development situation and experience of China's cyberspace security industry during the 12th Five-Year Plan period, and analyzes its new development trends. In addition, we propose policy suggestions for the industry development with the aim of providing a reference for China's cyberspace security industry during the 13th Five-Year Plan period.
Keywords: cyberspace security; cyberspace security industry; independence and controllability; standards

1. Introduction

A cyberspace, which acts as a conduit for online communication, is constructed from an interdependent network based on IT infrastructures. The cyberspace includes the Internet, telecommunications networks, computer systems, as well as the embedded processors, control devices, and others used in various industries. The term "cyberspace" is also commonly used to describe the overall digital environment of information organized around humans, machines, and matter, as well as the various interactions among them.

The goal of cyberspace security is to protect the cyberspace from network threats, whether accidental or perpetrated by attackers and to give the cyberspace the security capabilities of risk management, emergency response, quick recovery, and so on. Cyberspace security is designed to minimize cyberspace risks to an acceptable level. It comprises multiple security factors, not only including classic confidentiality, authentication, integrity, non-repudiation, availability, controllability, and other technology factors used in traditional information security, but also involving various tools, security management, security training and research, laws and regulations, technical standards, national strategies, and other factors used to protect network environments, organizations, and user assets [1].

The Ministry of Industry and Information Technology of the People's Republic of China issued *the Development Plan for Information Security Industry during the 12th Five-Year Plan Period*. This laid a solid foundation for extensively developing the cyberspace security industry in China. Research and development (R&D) on core technological products made some breakthroughs and numerous leading companies with indigenous intellectual property rights were established. Thus, an autonomously controllable industrial chain began to form [2]. Premier Li Keqiang proposed the concept of "mass entrepreneurship and innovation" at Summer Davos in September 2014, which generated considerable enthusiasm from China's enterprises in the cyberspace security industry. "Cyberspace Security" was declared a national first-level discipline in June 2015, which is expected to further improve the cyberspace security environment and to fill the enormous gaps of cyberspace security professionals in China. The first *Cyber Security Law (Draft)* was published in July 2015, stating that the cyberspace security has been promoted to the national strategic level [3]. These policy layouts reveal that China's network security industry has ushered in a major historic opportunity for development, and they lay a good foundation for developing the cyberspace security industry during the 13th Five-Year Plan period.

Received date: 2016-06-15; **revised date:** 2016-06-28
Author information: AN Da, China Academy of Electronics and Information Technology, engineers. His current research is strategic management, cyberspace security and scientific data. E-mail: andadk@163.com
Foundation item: CAE Major Advisory Project "Research on Promotion and Development Planning of China's Strategic Emerging Industries in the 13th Five-Year Plan Period (No. 2014-ZD-7)
Chinese version: Strategic Study of CAE 2016, 18 (4): 038–043
Cited item: An Da, Liang Zhihao, Xu Shouren. Study on the Development of Cyberspace Security Industry. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.04.006

2. Concept and scope of cyberspace security industry

Today, cyberspace is no longer merely a virtual space, but rather a common one for human activities. Everything that occurs in cyberspace is closely related to countries, nations, groups, and individuals. A network must be stable and secure in order to understand, utilize, and construct a cyberspace, while promoting its healthy and orderly development. The cyberspace security industry supports state network security, which can provide sustainable security technologies, security products, and security services for the national, enterprise, public, and other information systems.

As network technology continues to be developed, the environment related to cyberspace security has changed dramatically. First, the motives of network attackers have changed from simply brazen displays of technological sophistication to more utilitarian efforts designed to affect political, economic, and ideological factors. Second, network attackers have advanced technologies, powerful background, and abundant capital, which results in the transformation of their attacks from previously individual behaviors into those that are more organizational in scope. Third, network attacks have extended their scope from a generic network to a proprietary network. Fourth, big data, cloud computing, and other new generation information technologies also present unparalleled new challenges for cyberspace security, while simultaneously having a positive effect on the development of cyberspace industry. Cyberspace security industry involves many participants due to a wide range of internet information and the complex and changeable means in cyberspace security, including the providers of components, security chips, security system software, and development tools at the underlying level, the providers of security equipment and security application software at the intermediate level, and the providers of security integration and professional security services at the higher level. Currently, software and hardware product providers are still at the highest level of the industrial chain. However, with the changes to cyberspace security and the concept of security defense, the cyberspace security industry has changed from offering a single product to offering a complete security solution, and from offering software and hardware products to offering applications and services of security and protection.

3. Development of the cyberspace security industry

The Office of the Central Leading Group for Cyberspace Affairs was officially established in February 2014, and is personally chaired by General Secretary Xi Jinping. The Leading Group develops overall plans and coordinates all policies and other matters related to network security and informationization. The development of the cyberspace security industry receives powerful support from the policy-making environment. The issuance of the *Cybersecurity Law of the People's Republic of China (Draft)*in 2015 has enabled China to rapidly develop its network security laws and regulations. With a gradual optimized and ever-expanding industrial environment, breakthroughs in autonomously controllable technologies or products, and an increase in market shares, security systems and standardization have progressed remarkably.

3.1. Overall development of the cyberspace security industry

Faced with increasingly dangers related to cyberspace security, the major world powers have improved cyberspace security as a part of national strategy. As a result, competitions on cyberspace have been normalized among these countries. By contrast, major economic temptations have industrialized the organization of hackers, thus enabling them to conduct large-scale network hacks. Cyberspace security incidents now occur frequently, and important national information systems, enterprise information systems, and public privacy face critical security threats. Such threats have considerably catalyzed the development of global cyberspace security industry. The scale of the global information security industry reached 138.308 billion US dollars in 2014, representing an increase of 9.7% from the previous year (Table 1). Network supervision, information infrastructure safety protection, the construction of enterprise information security architectures, and data security have become the main impetus for development [4].

Although the cyberspace security industry in China started relatively late, its growth rate has been satisfactory. *The Development Plan for Information Security Industry during the 12th Five-Year Plan Period* was issued at the end of 2011. With it, information system demands for a national critical infrastructure, enterprise information systems, and network security for personal privacy have provided incentives for the rapid development of the cyberspace security industry. The industrial scale rose to 32.128 billion yuan in 2014, representing an increase of 21.0% from 2013 (Table 1) [4].

Table 1. The Scale and growth rate of cyberspace security industry from 2012–2014 [4].

	Scale and growth rate	2012	2013	2014
Globe	Sales (billion US dollars)	115.192	126.078	138.308
	Growth rate (%)	9.3	9.5	9.7
China	Sales (billion yuan)	21.640	26.552	32.128
	Growth rate (%)	20.9	22.7	21.0

3.2. Development of autonomously controllable industrial chain

China has been vigorously promoting innovation in the field of cyberspace security. In addition, having issued a series of polices related to the cyberspace security industry in 2014, the government has promoted the application of autonomously con-

trollable major hardware and software in the areas of banking, telecommunications, internet, and other industries and has established an long-term mechanism for autonomously controllable information technology, encouraging the government to adopt domestic operating systems that can gradually be deployed to commercial and civilian areas [5, 6].

A positive policy environment can promote the gradual perfection of an autonomously controllable industrial chain. Numerous leading enterprises have emerged from the areas of information infrastructure, basic software, information security products, application software, network security services, and other industries, such as Loongsun Technology Co., Ltd., Inspur Group Ltd, China Standard Software Co., Ltd., Venustech Co.Ltd, Westone Information Industry Co., Ltd., NSFOCUS Information Technology Co., Ltd., and Beijing VRV Software Co., Ltd. These enterprises are all focused on improving high-level indigenous intellectual property rights. Although a gap exists between similar domestic and foreign technologies or products, China's domestic products can basically replace foreign products. These enterprises are constantly developing and have in turn led to the development of certain industrial clusters. These enterprises have spontaneously developed an industrial alliance and formed a strategically cooperative organization to develop jointly, make their respective advantages complementary to each other, and share the benefits and risks. They have created an autonomously controllable industrial ecosystem in order to promote the sustainable development of an autonomously controllable industrial chain.

3.3. Development of cyberspace security technologies or products

With the development of the next generation of the information industry, cyberspace security technologies or products have gradually matured through constant innovation based on application demands. This innovation has been supported by national scientific and technological special projects.

In recent years, China has made considerable progress in the research and development (R&D) as well as industrial application of security chips, secure operating systems, and other basic technologies, especially cryptographic techniques, safety authority techniques, and trusted computing technologies. China’s Commercial encryption products and technical systems with indigenous intellectual property rights have matured basically, and China have owned a complete series of commercial encryption algorithms with high security in cryptographic techniques. The G-Cloud Technology and the Cloud Computing Center of China’s Academy of Science have developed the G-Cloud cloud operating system cooperatively. This system is designed for both government and business customers, which possesses indigenous intellectual property rights, and has obtained the highest security certification from the China Information Technology Security Evaluation Center. This represents a breakthrough for independent, secure, and controllable technical products in the field of cyberspace security.

3.4. Development of cyberspace security services

Cyberspace security represents a comprehensive problem, and the needs of state- and business-level users have transformed from single products into targeted and industry-oriented cyberspace security solutions. In addition, the industrial core value has changed from “products and technologies” to “applications and services.” The rate of security hardware to the cyberspace security products gradually decreased to 45.4% in 2014 globally, whereas the proportion of security software and security service products to the cyberspace security products was more than half (Table 2). By contrast, China's amount of security hardware still accounted for more than half that of the cyberspace security products over the same period, whereas the proportion of security service products was small, accounting for 8.7%. Therefore, there is a large gap between China's cyberspace security service industry scale and the global one which accounted for 20.4% in 2014 [4].

Table 2. Product mix of cyberspace security industry in 2014 [4]. %

	Hardware	Software	Service
Globe	45.4	34.2	20.4
China	54.3	37.0	8.7

3.5 Development of cyberspace security standards

Remarkable achievements in standardization of cyberspace security have occurred in China, which has gradually been integrated into international standardization systems. As of October 2014, the National Information Security Standardization Technical Committee has released 142 national standards covering information security fundamentals, security technologies and mechanisms, security management, security assessment, as well as confidentiality, cryptogram and communication security, and other security-related fields, all of which effectively protect national and social network security. Gradual improvement in the information security standardization system ensures that information security work, such as the network security management of cloud computing services, security checks of governmental information systems, hierarchical protection of information system security, testing of information security products and their authentication, and market access, has powerful technological support and a strong foundation [7].

4. Development issues and trends of the cyberspace security industry in China

4.1. Problems in the cyberspace security industry in China

4.1.1. Multi-channel management and decentralized responsibilities

China has established the Office of the Central Leading Group for Cyberspace Affairs. However, coordinating the work

is difficult because the field of cyberspace security involves many industries. In addition, China's cyberspace security industry employs a multi-departmental management, containing multiple departments. This has resulted in a decision-making power that is decentralized, as well as rule conflicts, low operational efficiency, difficult implementation, and difficulty in performing joint research on major cyberspace security issues and core security technologies. Therefore, the cyberspace security industry in China faces various challenges.

4.1.2. Industrial development lags behind demand growth

The Development Plan for Information Security Industry during the 12th Five-Year Plan Period revealed that China would establish 30 enterprises whose business income from information security could reach 100 million yuan by the end of the 12th Five-Year Plan period, and would also strive to cultivate backbone enterprises with a business income of 5 billion yuan from information security. However, achieve this objective is difficult because of the scale of existing backbone enterprises [2]. Currently, China has a shortage of specific enterprises dedicated to providing state-level users with cyberspace security services. In addition, China lacks both specialized cyberspace security enterprises that provide industrial solutions and complete product lines as well as leading enterprises to promote the development of the industrial cluster. Cyberspace security enterprises can still improve innovation of core technologies, products, and services. The technologies in the major links of the industrial chain still need to be brook through.

4.1.3. Considerable work is required for autonomously controllable products to become popular

At present, China must rely on foreign products for most high-end components and core network equipment for information systems in critical areas. For example, the central departments of the party, government, and army contain few domestic information security management systems, operating systems, databases, servers, and other equipment. Autonomously controllable software and hardware have not yet gained wide popularity and recognition, indicating considerable work is required to popularize application. Realizing independent breakthroughs in the core software and hardware applied in the system have become the strategic objective that must be conquered. Compared to foreign similar products, the domestic autonomously controllable hardware and software products need to be improved with respect to technologies, product stability, compatibility, technical specifications, and standardization. Therefore, the work for localization and substitution based on independence and controllability continues to face arduous tasks.

4.1.4. Cyberspace security service industry must be perfected

China attaches great importance to the cyberspace security service industry, and traditional security enterprises in combination with their own technical features have accelerated the transition from security hardware and security software providers to security service providers. However, China's cyberspace security service systems are incomplete without standards. Thus, the security service industry remains the weak link in the cyberspace security industry. China not only have a shortage of high-quality specialized security providers of considerable scale, but also lack many related professionals. Therefore, the systematic construction of the cyberspace security service industry is very slow.

4.1.5. Industrial environment must be improved

"Cyberspace Security" has been declared a national first-level discipline, and the *Cybersecurity Law of the People's Republic of China(Draft)* has been published in China. These are expected to complement China's demands for high-level and interdisciplinary professionals related to the cyberspace security to ensure that cyberspace security practices are properly followed. However, current policies and regulations fall short of innovation and intellectual property protection, and vicious competition among enterprises is common. Therefore, the environment for developing the cyberspace security industry must be improved.

4.2. Development trends in cyberspace security industry during the 13th Five-Year Plan period

4.2.1 Overall development trends of cyberspace security industry

Faced with increasingly serious threats and challenges, China's government has given high priority to developing the cyberspace security industry. It strengthens the construction of cyberspace security for critical information systems in telecommunications, finance, energy, and other national critical infrastructures, which allows domestic products to replace with foreign products used in critical fields of the cyberspace security, gradually diversifies independent innovative products, and thus continuously increases the scale of the cyberspace security industry. Table 3 reveals that the scale of China's cyberspace security industry will be up to 61.987 billion yuan by 2017. In addition, cyberspace security industry will remain dominated by network equipment and other hardware information security infrastructures, and segmented industries of software and service will experience certain growth (Table 4) [4].

4.2.2. Wide integration of cyberspace security and new generation of information technology

Mobile internet has become the new battlefield of cyberspace security. Mobile internet security is primarily concerned with the security of mobile equipment, mobile applications, and mobile environments. The polices of the Ministry of Industry and Information Technology of the People's Republic of China focus on the security management for mobile application store and application program, including urging the application store to establish the management systems such as ID authentication

Table 3. Predictions for scale and growth rate of China's information security industry from 2015–2017 [4].

Year	2015	2016	2017
Market Size (billion yuan)	39.839	50.396	61.987
Growth Rate (%)	24.0	26.5	23.0

Table 4. Predictions for percentages of product mix of China's information security industry from 2015–2017 [4]. %

Year	Hardware	Software	Service
2015	53.2	38.4	8.4
2016	52.9	38.6	8.5
2017	51.9	39.1	9.0

for program developers, security checks of application program, withdrawing and blacklisting malicious program, user supervision and report, and so on, as well as to establish and perfect a third-party security inspection mechanism for mobile application programs [5]. Mobile Internet provides new opportunities for developing the cyberspace security industry with respect to "cloud computing + smart terminal". On the one hand, a huge amount of private information from users is gathered on the cloud, which generates considerable demand for cloud security products and services. On the other hand, because the functionality of mobile terminals (storage, positioning, photographing) is constantly improving and has considerably enhanced the user ability to obtain and share information, the supervision on user has become increasingly difficult. Therefore, this provides major opportunities for the creation of products and services that influence public opinion about the mobile internet.

Cyberspace security and big data mutually support each other. The extensive application of big data technology has created new types of cyberspace security products. One type of these products refers to utilizing big data technology for security defense, including a passive defense against the network, terminals, database, applications, identification data, and the data of and access management systems; an active defense against potential attacks; and security big data collection system used to identify the attacking behavior. Another type of cyberspace security products is used to ensure the safe application of big data, including open data environment security and unstructured data storage security.

4.2.3. Cyberspace security and *Made in China 2025*

Made in China 2025 is China's version of "Industry 4.0", which proposes a "three-step" strategy to transform China into a manufacturing power within three decades. This strategy is based on major changes in the patterns of the global manufacturing industry, as well as our own economic development environment. The program of action for the first decade proposes five priorities: improving innovation in China's manufacturing industry, integrating informationization and industrialization, strengthening the nation's basic industrial capacity, improving the construction of quality brands, and fully implementing green manufacturing [8].

The cyberspace security industry is the new generation of the information technology industry, and is vigorously promoted by the strategy of *Made in China 2025*. Developing the cyberspace security industry is not only an important task for the strategy of *Made in China 2025*, but also an important guarantee to realize this strategy, as described in the following subsection.

4.2.3.1. Cyberspace security is the key to realizing independence and controllability

Currently, domestic autonomously controllable information systems have made technological breakthroughs with respect to processors, operating systems, databases, middleware, and other major technologies. Adapting, testing, and validating between hardware and software are currently being fully conducted, and the large-scale applications of the domestic systems is being implementing within a certain range. However, current autonomously controllable information systems lag behind in standardization, serialization, and generalization, and the autonomously controllable industry lacks standards and norms to support. Software and hardware are being developed independently of one another without sufficient technological synergy and integration. This means that underlying hardware and upper software are not sufficiently integrated and optimized. These problems lead to system vulnerabilities and higher security risks. Therefore, it is necessary to conduct independent R&D of core technological products for cyberspace security and vigorously strengthen integrated system security design. Simultaneously, China should also develop the cyberspace security service industry and provide testing and evaluation, monitoring and early warning, security maintenance, and other high-quality professional services for the autonomously controllable information systems.

4.2.3.2. Cyberspace security strengthens basic industrial capabilities

Integration of informationization and industrialization represents the general direction of development. Smart manufacturing is one of the focus in the integration of informationization and industrialization. New production modes will gradually realize an intelligentized production process. However, cyberspace security issues are becoming increasingly more serious, and are now a central focus of all aspects of enterprises, including its R&D, production, management, and services. In addition, the application of the Internet to manufacturing has normalized threats to cyberspace. In order to strengthen our industrial base capacity and break the foreign monopoly, *Made in China 2025* proposes a plan to develop core basic parts and components, advanced basic techniques, basic materials, and an industrial technological base. However, high-level production lines for many core components, such as chip manufacturing, have been established abroad. These

components may have been embedded into the back doors and will suffer from cyberspace attacks during production. Therefore, China should consider an integrated design of cyberspace security when promoting the development of the "Four Basics" as specified in *Made in China 2025*.

4.2.3.3. Improve the brand value of cyberspace security enterprises in China

The strategy of *Made in China 2025* encourages China's enterprises to pursue superior quality, create famous-brand products having indigenous intellectual property rights, and improve the brand value of enterprise all as a means of improving and the overall image of Made in China. In recent years, the cyberspace security industry has become prosperous, and associated enterprises have been divided by market competition mechanism. Those cyberspace security enterprises that own the core technological products and services have a lead position in the markets, whereas poorly run enterprises have been eliminated. Thus industrial patterns have become clear. Additionally, the mass fervor for innovation and entrepreneurship has resulted in expanded development space for the Internet and thus provides more opportunities for cyberspace security industry. In recent years, the traditional Internet giants such as China's Tencent, Alibaba, and Baidu have begun to establish the cyberspace security industry by becoming shareholders or acquiring medium- and small-sized information security enterprises. China's Huawei and other equipment providers have also taken advantage of their technological R&D for network equipment and software and hardware products to develop the products related to network security. The brand effect of these leading enterprises and their market capacity are conducive to promoting cyberspace security products. This can be regarded as a means to establish industrial brands for cyberspace security in China.

5. Policy suggestions for promoting the cyberspace security industry

5.1. Consolidate strategic planning for national industries and build a powerful cyberspace security base

China must unify in terms of industrial strategic planning and comprehensively consider establishing a high-level, autonomously controllable, and powerful cyberspace security industrial base. The development of national industrial teams for cyberspace security should be supported with the aid of China's government. First, it is necessary to achieve breakthroughs in core information technologies or products, improve the capacity to protect against cyberspace security threats, and gradually eliminate passive situation in technologies or products restrained by other countries. Second, China's government should strengthen its support policies for autonomously controllable industries and cannot rely solely on the market regarding the core areas related to national security. Instead, the government must establish macro-control and even phased support, focusing on supporting leading domestic enterprises to improve the strategic position of the cyberspace security market in China, so that China's cyberspace security enterprises can enter the international market while remaining strongly rooted in China's markets.

5.2. Establish chief security officer for cyberspace and implement policies and measures for cyberspace security industry

"Responsibility Implementation" is the prerequisite for implementing policies and measures of the cyberspace security industry. For example, the *Cybersecurity Law of the People's Republic of China (Draft)* specifies establishing a cyberspace security duty officer and responsibility system. Therefore, it is important to establish the Chief Security Officer of cyberspace and in turn define the security and responsibility system so that the policies and measures for the cyberspace security industry can be "specific to the position and the individual".

5.3. Accelerate standardization of cyberspace security standards

China should formulate cyberspace security standards as soon as possible, further improve standard quality, and address both new and common problems based on the current and future development trends in cyberspace security. All governments departments should actively work to ensure standard quality by improving standardization, strengthening the management on the standards' study and formulation, and intensifying the support to major standards. In addition, the governments should also establish standard evaluations, and consider the participation of the public and experts as standard evaluation basis to increase the accepted and influence level of China's standards.

References

[1] Liu Z R. Information security industry is the guarantee of sustainable development of information security industry [J]. Information Security and Communication Privacy, 2002 (7): 15–18. Chinese.

[2] The Information Technology and Software Service Division of the Ministry of Industry and Information Technology of the People's Republic of China. Promote the innovation and development of the industry, enhance the ability of information security—interpretation of *the development plan for information security industry during the 12th Five-Year Plan period* [N/OL]. China Electronics News. (2012-02-24) [2016-06-15]. http://epaper. cena.com.cn/content/2012-02/24/content_233661.htm. Chinese.

[3] The Legislative Affairs Committee of the Standing Committee of the National People's Congress. *Cybersecurity Law of People's Republic of China (Draft)* [EB/OL]. (2015-07-06) [2016-06-15]. http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm. Chinese.

[4] China Center for Information Industry Development. Annual report on the development of information security industry in China (2014-2015) [R/OL]. (2015-02-10) [2016-06-15]. http://www.ccidreport.com/report/content/6/201502/679308.html. Chinese.

[5] The Ministry of Industry and Information Technology of the People's Republic of China. Guidance on strengthening cyberspace security in the telecommunications and internet industries [EB/OL]. (2014-08-29) [2016-06-15]. http://www.gov.cn/xinwen/2014-08/29/content_2742159.htm. Chinese.

[6] China Banking Regulatory Commission. Guidance on strengthening the construction of cyberspace and informationization in banking industry by applying safe and controllable information technologies [EB/OL]. (2014-09-03) [2016-06-15]. http://www.cbrc.gov.cn/govView_115696B8621049099A0B880DAB133A33.html. Chinese.

[7] Gao L. Standardization supports cyberspace security assurance vigorously [J]. Information Security and Communication Privacy, 2014 (12): 49–50. Chinese.

[8] The State Council of the People's Republic of China. Notice of the State Council on issuing *Made in China 2025* [EB/OL]. (2015-05-19) [2016-06-15]. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm. Chinese.